(19) (11) Publication number: 09212457 A

Generated Document.

PATENT ABSTRACTS OF JAPAN

(21) Application number: 08014221

(51) Intl. Cl.: G06F 15/00 G06F 13/00 G09C 1/00 G09C 1/00 G09C 1/00 H04H 1/02 H04L 9/08 H04L 9/32 H04N 7/14 H04N 7/167

(22) Application date: 30.01.96

(30) Priority:

(43) Date of application publication: 15.08.97

(84) Designated contracting states:

(71) Applicant: MITSUBISHI ELECTRIC CORP

(72) Inventor: OGAWA AKI

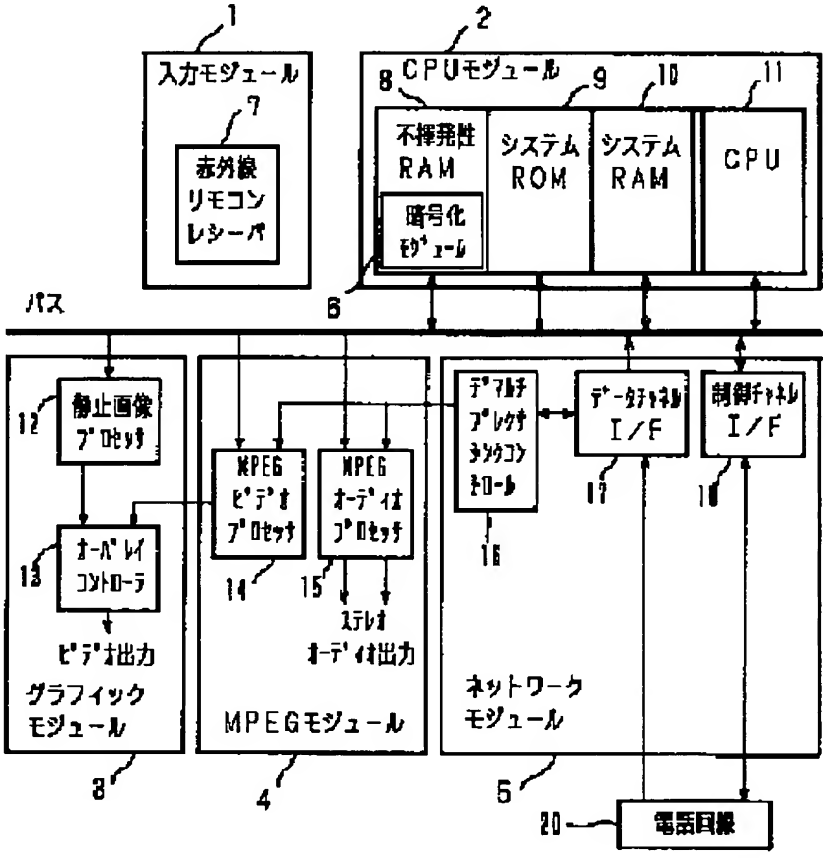
(74) Representative:

(54) CIPHERING AND DECIPHERING DEVICE OF DIGITAL BIDIRECTIONAL COMMUNICATION TERMINAL

(57) Abstract:

PROBLEM TO BE SOLVED: To keep the price of a digital bilateral communication terminal main body low by adding a ciphering, a deciphering, and a user authenticating function to a digital bilateral communication terminal, and then actualizing services which require security like credit card payment by bilateral CATV and further not incorporating the ciphering function originally, but downloading a ciphering module from a server.

SOLUTION: The digital bilateral communication terminal is connected to the server through a public telephone line or leased line and has a system ROM 9, a system RAM 10, and a nonvolatile RAM 8 inside and also has an operating system based upon OS/9. The digital bilateral communication terminal downloads modules for ciphering and deciphering data from the server, saves the downloaded ciphering module in the system RAM 10, and uses ciphering for the subsequent transmission and reception of data.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－212457

(43)公開日　平成９年(1997)８月15日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	15/00	３３０		Ｇ０６Ｆ	15/00	３３０Ａ
	13/00	３５１			13/00	３５１Ｈ
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｃ
			7259－5Ｊ			６３０Ｅ
		６４０	7259－5Ｊ			６４０Ｂ

審査請求　未請求　請求項の数６　ＯＬ　（全 49 頁）　最終頁に続く

(21)出願番号　特願平8－14221

(22)出願日　平成８年(1996)１月30日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　小川　亜紀
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

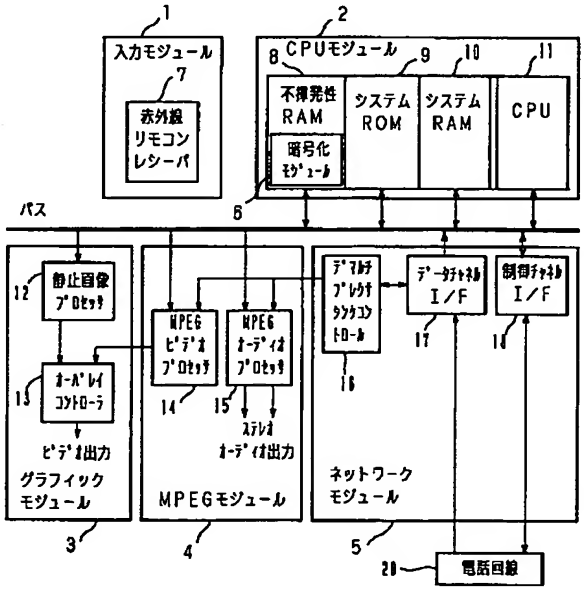
(74)代理人　弁理士　宮田　金雄　（外３名）

(54)【発明の名称】　デジタル双方向通信端末における暗号化・復号化装置

(57)【要約】

【課題】　デジタル双方向通信端末において、デジタル双方向通信端末に暗号化、復号化およびユーザーの認証機能を付加することにより、双方向ＣＡＴＶによるクレジットカード支払い等のセキュリティを要するサービスの実現を可能とし、更に暗号化機能を初めから組み込むのではなく、暗号化モジュールをサーバからダウンロードさせることによって、デジタル双方向通信端末本体の価格を低く押さえることを可能とする。

【解決手段】　デジタル双方向通信端末は、公衆回線または専用線を通じてサーバに接続され内部にシステムＲＯＭ、システムＲＡＭ、不揮発性ＲＡＭを有し、ＯＳ／９を核とするオペレーティングシステムを持つ。デジタル双方向通信端末はサーバよりデータの暗号化、復号化のためのモジュールをダウンロードし、ダウンロードした暗号化モジュールをシステムＲＡＭに保存し、それ以降のデータの授受に暗号を使用する機能を有する。



【特許請求の範囲】

【請求項１】　公衆回線または専用線を通じて双方向通信サービスプロバイダによって提供されるサービス提供装置もしくは構内に閉じたシステムにおけるサービス提供装置（以下サーバ）に接続され、内部にＲＯＭ、不揮発性ＲＡＭとＲＡＭを有し、ＯＳ／９（登録商標）を核とするオペレーティングシステムを持つデジタル双方向通信端末において、ドライバまたはアプリケーションはＳ／Ｗプログラムであり、特にＣＲＣチェックコードを有する実行モジュール（以下、Ｓ／Ｗモジュール）であって、あらかじめ前記ＲＯＭに格納されているか、もしくはサーバよりダウンロードされ前記ＲＡＭに記憶され、初期化・リンクされることによって使用可能となるものであり、前記デジタル双方向通信端末が前記サーバからダウンロードし、前記ＲＡＭに格納し、前記デジタル双方向通信端末と前記サーバ間で授受されるデータの暗号化、復号化機能を実現することを特徴とするデジタル双方向通信端末における暗号化・復号化装置。

【請求項２】　公衆回線または専用線を通じて双方向通信サービスプロバイダによって提供されるサービス提供装置もしくは構内に閉じたシステムにおけるサービス提供装置（以下サーバ）に接続され、内部にＲＯＭ、不揮発性ＲＡＭとＲＡＭを有し、ＯＳ／９を核とするオペレーティングシステムを持ち、Ｈ／Ｗによるデータの認証装置を有するデジタル双方向通信端末において、ドライバまたはアプリケーションはＳ／Ｗプログラムであり、特にＣＲＣチェックコードを有する実行モジュール（以下、Ｓ／Ｗモジュール）であって、あらかじめ前記ＲＯＭに格納されているか、もしくはサーバよりダウンロードされ前記ＲＡＭに記憶され、初期化・リンクされることによって使用可能となるものであり、前記デジタル双方向通信端末が前記サーバからダウンロードし、前記ＲＡＭに格納し、前記デジタル双方向通信端末と前記サーバ間で授受されるデータの暗号化、復号化機能を実現し、前記認証装置によって、データの認証を行うことを特徴とするデジタル双方向通信端末における暗号化・復号化装置。

【請求項３】　公衆回線または専用線を通じて双方向通信サービスプロバイダによって提供されるサービス提供装置もしくは構内に閉じたシステムにおけるサービス提供装置（以下サーバ）に接続され、内部にＲＯＭ、不揮発性ＲＡＭとＲＡＭを有し、ＯＳ／９を核とするオペレーティングシステムを持ち、前記ＲＯＭ内にデータの認証機能を実現するモジュール（以下、認証モジュール）を有するデジタル双方向通信端末において、ドライバまたはアプリケーションはＳ／Ｗプログラムであり、特にＣＲＣチェックコードを有する実行モジュール（以下、Ｓ／Ｗモジュール）であって、あらかじめ前記ＲＯＭに格納されているか、もしくはサーバよりダウンロードされ前記ＲＡＭに記憶され、初期化・リンクされることによって使用可能となるものであり、前記デジタル双方向通信端末が前記サーバからダウンロードし、前記ＲＡＭに格納し、前記デジタル双方向通信端末と前記サーバ間で授受されるデータの暗号化、復号化機能を実現し、前記認証モジュールによって、データの認証を行うことを特徴とするデジタル双方向通信端末における暗号化・復号化装置。

【請求項４】　公衆回線または専用線を通じて双方向通信サービスプロバイダによって提供されるサービス提供装置もしくは構内に閉じたシステムにおけるサービス提供装置（以下サーバ）に接続され、内部にＲＯＭ、不揮発性ＲＡＭとＲＡＭを有し、ＯＳ／９を核とするオペレーティングシステムを持ち、前記ＲＯＭ内にデータの認証機能を実現するモジュール（以下、認証モジュール）を有するデジタル双方向通信端末において、ドライバまたはアプリケーションはＳ／Ｗプログラムであり、特にＣＲＣチェックコードを有する実行モジュール（以下、Ｓ／Ｗモジュール）であって、あらかじめ前記ＲＯＭに格納されているか、もしくはサーバよりダウンロードされ前記ＲＡＭに記憶され、初期化・リンクされることによって使用可能となるものであり、暗号化・復号化機能は、前記デジタル双方向通信端末が前記サーバからダウンロードし、前記ＲＡＭに格納し、前記デジタル双方向通信端末と前記サーバ間で授受されるユーザによる入力によって選択されたデータの暗号化、復号化機能を実現することを特徴とするデジタル双方向通信端末における暗号化・復号化装置。

【請求項５】　公衆回線または専用線を通じて双方向通信サービスプロバイダによって提供されるサービス提供装置もしくは構内に閉じたシステムにおけるサービス提供装置（以下サーバ）に接続され、内部にＲＯＭ、不揮発性ＲＡＭとＲＡＭを有し、ＯＳ／９を核とするオペレーティングシステムを持ち、前記ＲＯＭ内にデータの認証機能を実現するモジュール（以下、認証モジュール）を有するデジタル双方向通信端末において、ドライバまたはアプリケーションはＳ／Ｗプログラムであり、特にＣＲＣチェックコードを有する実行モジュール（以下、Ｓ／Ｗモジュール）であって、あらかじめ前記ＲＯＭに格納されているか、もしくはサーバよりダウンロードされ前記ＲＡＭに記憶され、初期化・リンクされることによって使用可能となるものであり、暗号化・復号化機能は、前記デジタル双方向通信端末が前記サーバからダウンロードし、前記ＲＡＭに格納し、前記サーバから前記デジタル双方向通信端末にダウンロードされた暗号化適用データリストに含まれるデータが前記デジタル双方向通信端末と前記サーバ間で授受される際の暗号化、復号化機能を実現することを特徴とするデジタル双方向通信端末における暗号化・復号化装置。

【請求項６】　公衆回線または専用線を通じて双方向通信サービスプロバイダによって提供されるサービス提供

装置もしくは構内に閉じたシステムにおけるサービス提供装置（以下サーバ）に接続され、内部にＲＯＭ、不揮発性ＲＡＭとＲＡＭを有し、ＯＳ／９を核とするオペレーティングシステムを持ち、前記ＲＯＭ内にデータの認証機能を実現するモジュール（以下、認証モジュール）を有するデジタル双方向通信端末において、ドライバまたはアプリケーションはＳ／Ｗプログラムであり、特にＣＲＣチェックコードを有する実行モジュール（以下、Ｓ／Ｗモジュール）であって、あらかじめ前記ＲＯＭに格納されているか、もしくはサーバよりダウンロードされ前記ＲＡＭに記憶され、初期化・リンクされることによって使用可能となるものであり、暗号化・復号化機能は、前記デジタル双方向通信端末が前記サーバからダウンロードし、前記ＲＡＭに格納し、データが前記デジタル双方向通信端末と前記サーバ間で授受される際の暗号化、復号化機能を実現し、一度暗号化したデータの暗号化形式を前記ＲＡＭ内に保持し、同じデータの送信時には記憶されたデータを使用する機能を有することを特徴とするデジタル双方向通信端末における暗号化・復号化装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はデジタル双方向通信端末にセキュリティ機能を付加するものであり、特にＯＳ／９のモジュール形式と、双方向ＣＡＴＶシステムにおけるデータのダウンロード機能を利用して、暗号化機能を実現するデジタル双方向通信端末に関するものである。

【０００２】

【従来の技術】デジタル双方向通信端末用ＯＳとしてＯＳ／９を核としたＤＡＶＩＤが発表されており、デジタル双方向通信端末を構成する最小限のモジュールによる構成とその拡張は既にＤＡＶＩＤシステムとして発表されている。ＤＡＶＩＤと一般的なＳＴＢの構造は日経バイト１９９５．９月号で解説されている。従来のデジタル双方向通信端末の構成と動作の詳細は後に記述する。しかし、ＤＡＶＩＤを含む典型的なデジタル双方向通信端末の構成には暗号化機能は含まれていない。拡張として暗号・条件付きアクセスの実現が取り上げられているが、ここでのセキュリティ機能は暗号化のためのＨ／ＷとＨ／Ｗに対応するドライバを組み込むことで実現されるものである。

【０００３】従来のＣＡＴＶシステムのセンターのサーバと端末装置とのデータの送受信方式については、特開昭５７－６５９８２号公報および特表平６－５０１６０１号公報に記述されているが、ここで送受信されるデータは暗号化が施されたものではなく、データに識別のためのコードを付加し、平文のままデータを流すものである。ＣＡＴＶシステムにおけるセキュリティとしては、ダウンロードされたブーターイメージに含まれたデータから計算されたブーターチェックサムとプログラムのタグ信号から検出された有効チェックサムを比較し、一致すればデスクランブルが作動し、受信されるべきプログラムが視聴のためデスクランブルされる方式は特開昭６３－２６０９３号公報に記述されている。しかし、これはサーバから流れるデータを正当な視聴者にのみ受信可能となるよう視聴者を制限するためのものであり、視聴者側かのデータを保護するものではない。デジタル双方向通信端末において、双方向のデータを暗号化し、データ保護を実現するためには、暗号化・復号化装置が必要となる。

【０００４】図４０はＯＳ／９を核とした一般のデジタル双方向通信端末の構成図である。図５において、１から５はそれぞれデジタル双方向通信端末におけるモジュールである。モジュールとは、ハードウェアとソフトウェアの組み合わせによって、デジタル双方向通信端末において各機能を実現するための構成要素であり、各モジュール間をバスを通じて制御信号、またはデータを送受信することによって、デジタル双方向通信端末を動作させるものである。以下、図４０の構成要素を説明する。入力モジュール１、ＣＰＵモジュール２、グラフィックモジュール３、ＭＰＥＧモジュール４、ネットワークモジュール５はそれぞれバスに接続されており、ＭＰＥＧモジュール４はネットワークモジュール５の後段に配し、グラフィックモジュール３の前段に配している。入力モジュール１はユーザからの入力を受け付け、デジタル双方向通信端末内部に入力信号を取り込み、ＣＰＵへ信号送信を行うモジュールである。ＣＰＵモジュール２は中央処理装置と記憶装置からなるデジタル双方向通信端末内部の各モジュールからの信号を受け付け、受け付けた信号を処理し、必要なモジュールへ動作命令の出力を行い、それぞれのモジュールの制御を行うモジュールである。グラフィックモジュール３はサーバからダウンロードされた静止画像をビデオ出力可能な形式にデータ処理を行い、ビデオ出力へ出力させることと、ＭＰＥＧモジュールから送られてきたデータをビデオ出力へ出力させることと、静止画像と動画像の重ね合わせ処理を行い、ビデオ出力へ出力させるモジュールである。ＭＰＥＧモジュール４はネットワークモジュールより受信したサーバからダウンロードされたＭＰＥＧデータの復号を行い、オーディオデータをオーディオ出力に出力させることと、ビデオデータをグラフィックモジュールへ送信するモジュールである。ネットワークモジュール５はネットワークに接続され、ネットワークからデータを受信し、受信データを動画像・静止画像に分解し、更に動画については音声データとビデオデータに分解したあと、ＭＰＥＧモジュールへデータを送信する処理を行うモジュールである。入力モジュールには、赤外線リモコンレシーバ７が含まれる。このレシーバによって、ユーザのリモコン操作による入力を受信し、デジタル双方向通信

端末へ取り込むことを可能とする。ＣＰＵモジュールにはＣＰＵ１１、不揮発性ＲＡＭ８、システムＲＯＭ９、システムＲＡＭ１０が存在する。ＣＰＵはデジタル双方向通信端末に取り込まれる信号を解析し、その解析結果に基づいて各モジュールへ動作命令信号を送信する。システムＲＯＭは、デジタル双方向通信端末本体に予め組み込まれるソフトウエアモジュールが記憶される。

【０００５】図３７に示すようにシステムＲＯＭには、ＯＳ－９のＫｅｒｎｅｌ２６、Ｉ／Ｏマネージャ２７、デバイスドライバ２８、ＡＰＩおよびプロトコル２９が組み込まれ、アプリケーション領域３０に、拡張されたアプリケーションモジュールを格納させることが可能である。システムＲＡＭ１０および不揮発性ＲＡＭ８には、ＳＴＢの起動後にサーバからダウンロードされたデバイスドライバ、アプリケーション、データが記録される。グラフィックモジュールには、静止画像データを出力可能な形式に処理する静止画像プロセッサ１２と、静止画像と、ビデオデータを取り込んで、重ね合わせなどの処理を行い、ビデオ出力に出力させるオーバレイコントローラ１３が含まれる。ＭＰＥＧモジュールには、ビデオデータとオーディオデータに切り分けられたＭＰＥＧデータのうち、ビデオデータを復号し、グラフィックモジュール内のオーバレイコントローラへ引き渡すＭＰＥＧビデオプロセッサ１４と、オーディオデータを復号し、ステレオオーディオ出力に出力するＭＰＥＧオーディオプロセッサ１５が含まれる。ネットワークモジュールには高帯域単方向回線に接続され、サーバからダウンロードされる画像データおよび音声データなどのデータを受信するためのデータチャネルＩ／Ｆ１７と、低帯域双方向回線とに接続され、通信制御を行うための信号を送受信し、デジタル双方向通信端末からサーバへの要求信号を送信し、サーバからの制御信号を受信するための制御チャネルＩ／Ｆ１８と、データチャネルＩ／Ｆ１７とデータの送受信を行い、ＭＰＥＧデータのビデオデータとオーディオデータの切り分けを行い、ＭＰＥＧオーディオプロセッサ１５とＭＰＥＧビデオプロセッサ１４への送信を行うデマルチプレクサシンクコントロール１６が存在する。

【０００６】次に、図４０に示すデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。図３８は電源ＯＮ時のデジタル双方向通信端末の動作フローチャートである。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、Ｋｅｒｎｅｌの立ち上げを実行する。Ｋｅｒｎｅｌの立ち上げが終了した状態で、電源ＯＮ動作が完了する。

【０００７】次に、ユーザからデータダウンロードのための選択信号入力があったときの動作を説明する。図３９はデータダウンロード時のデジタル双方向通信端末の動作フローチャートである。入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、ネットワークモジュール５へダウンロード命令とダウンロードすべきデータ名を受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、データチャネルＩ／Ｆ１７を通じて、サーバからデータをダウンロードする。ダウンロードされたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上、従来のＯＳ／９を核とした採用したデジタル双方向通信端末の動作を説明した。

【０００８】

【発明が解決しようとする課題】上述した従来技術におけるネットワークセキュリティ技術はコンピュータネットワークにおける技術であり、双方向ＣＡＴＶシステムにおいてはまだ確立されていない。　また、インターネット接続を実現するＣＡＴＶにおいて、ケーブルモデムにセキュリティ機能を実装することが計画されているが、ケーブルモデムによるセキュリティ機能の実現であり、デジタル双方向通信端末そのものにセキュリティ機能を実装するものではなく、双方向ＣＡＴＶシステム単独でのセキュリティ機能ではない。しかし、オンライン

・ショッピングや銀行口座の残高照会といったサービスの提供を実現するためには双方向ＣＡＴＶシステムにおけるセキュリティ確保は必修条件である。双方向ＣＡＴＶでも、暗号化技術をとりいれたデジタル双方向通信端末を実現することによって、サーバ・端末間で送受信されるデータのセキュリティを確保することが可能であり、提供可能なサービスの幅を広げることができる。ＤＡＶＩＤの拡張としてセキュリティ機能が挙げられているが、これは暗号化のためのＨ／ＷとＨ／Ｗに対応するためのドライバを組み込むことによってデジタル双方向通信端末にセキュリティ機能を実現するものであり、デジタル双方向通信端末のＨ／Ｗ構成の変更を要し、一度組み込まれた暗号か方式を変更するためには更にＨ／Ｗの変更を必要とするものであり、暗号化のためのコストが高くなるという課題を有するものである。

【０００９】本発明は上記のような課題を解決するためになされたもので、特にデジタル双方向通信端末にＨ／Ｗによるセキュリティ機能を組み込むのではなく、暗号化のためのアプリケーションモジュールとしてサーバからダウンロードさせることによって、暗号化機能付加のためのコストを軽減し、また暗号化機能の更新を容易に実現することができるデジタル双方向通信端末における暗号化・複号化装置を得ることを目的とする。

【００１０】

【課題を解決するための手段】双方向ＣＡＴＶシステムにおける暗号化機能を実現するため、デジタル双方向通信端末に暗号化機能を実装する。暗号化機能としては、ＤＥＳ暗号に代表される秘密鍵暗号方式と、ＲＳＡに代表される公開鍵暗号方式を組み合わせた方式を用いるものとする。秘密鍵暗号方式とは、暗号化と復号化に用いる鍵が共通であり、暗号化に用いられた鍵を用いて暗号化アルゴリズムを逆に実行することによって、復号を行い、暗号化を施す前の原文を得るものである。この方式は、単純な排他的論理和の繰り返しアルゴリズムで実現されるもので、高速な処理を可能とする反面、送信側と受信側で共通の鍵を保有する必要があり、鍵の配送・保持が困難であるという欠点を有する。公開鍵暗号方式とは、落とし戸関数と呼ばれる一方向には容易に実行でき、逆数を求めるのは非常に困難である関数を利用するもので、暗号化と復号化に使用する鍵が異なるものである。したがって、鍵の配送・保持は容易に行える反面、秘密鍵暗号方式に比べて計算が複雑であり、秘密鍵暗号方式と比較して暗号化・復号化に処理時間を要するという欠点を有する。ただし、公開鍵暗号方式を使用して、認証及び鍵配送を行い、データの暗号化は秘密鍵暗号によって行うことによって、それぞれの利点を生かして使用することが可能となる。本発明に係るデジタル双方向通信端末における暗号化・復号化装置は、双方向ＣＡＴＶのデータダウンロード機能を活用し、暗号化のためのＳ／Ｗモジュールをサーバからダウンロードすることにより、デジタル双方向通信端末に暗号化機能を組み込むとともに、モジュールをリンクし、デジタル双方向通信端末における暗号化機能を実現するものである。ＯＳ／９はデバイスドライバからアプリケーションに至るまで実行プログラムがそれぞれモジュールとなっており、それらモジュールをメモリにロードし、リンクすることにより、各種の機能をダイナミックに実行可能にすることができる特徴を持っている。このようなＯＳ／９を核とするデジタル双方向通信端末では、各種の機能を実現するためのモジュールを予めＲＯＭに記憶させておく以外に、モジュールをサーバからダウンロードすることによってモジュールの機能をデジタル双方向通信端末に付加することが可能である。モジュールのダウンロードは通常デジタル双方向通信端末がサーバからオーディオデータ、ビデオデータ等をダウンロードするための回線を使用し、ＯＳ／９を核とするデジタル双方向通信端末のために開発されたデータのダウロードプロトコル、UPLINK/DOWNLINK API を使用する。デジタル双方向通信端末にはこのプロトコルモジュールを実装する。このダウンロードプロトコルは、サーバ用にはＣライブラリが存在しており、任意のＯＳ上で動作する。したがって、UPLINK/DOWNLINK プロトコルを使用した任意のＯＳを使用するサーバからのデータのダウンロードが可能である。

【００１１】また、双方向ＣＡＴＶのデータダウンロード機能を活用し、暗号化のためのＳ／Ｗモジュールをサーバからダウンロードするとともに認証機能のためのＨ／Ｗを付加し、Ｈ／Ｗ認証装置のためのドライバをＲＯＭに組み込むものである。

【００１２】また、双方向ＣＡＴＶのデータダウンロード機能を活用し、暗号化のためのＳ／Ｗモジュールをサーバからダウンロードするとともに、認証機能実現のための手段として、認証のためのＳ／Ｗモジュールは組み込みモジュールとしてＲＯＭに組み込むものである。

【００１３】また、双方向ＣＡＴＶのデータダウンロード機能を活用し、暗号化のためのＳ／Ｗモジュールをサーバからダウンロードするとともに、ユーザの選択を受信するための手段として、リモコンを使用し、入力モジュールに暗号化を行うかどうかの選択信号を入力するための機能と、受信した選択信号をＣＰＵモジュールに伝えるための機能を付加し、ＣＰＵモジュールのＲＡＭ領域に、選択信号を格納するための領域を確保するものである。

【００１４】また、サーバからダウンロードしたリストを参照して選択的に暗号化を行うための手段として、双方向ＣＡＴＶのデータダウンロード機能を活用し、暗号化適用データのリストを参照して選択的に暗号化を行う機能を付加した暗号化のためのＳ／Ｗモジュールをサーバからダウンロードするとともにサーバから暗号化適用データのリストをダウンロードする機能と、暗号化適用データのリストを格納するための領域をＲＡＭ領域に設

けることとしたものである。

【００１５】また、一度暗号化を実行したデータの暗号化形式を記憶し、同じデータの送信時に記憶されたデータを使用するために、双方向ＣＡＴＶのデータダウンロード機能を活用し、暗号化データのリストを参照し、暗号化データが存在しない場合にのみ選択的に暗号化を行う機能を付加した暗号化のためのＳ／Ｗモジュールをサーバからダウンロードするとともに、暗号化データの保存のための領域をＲＡＭ領域に設けることとしたものである。

【００１６】

【発明の実施の形態】本発明の実施の形態であるデジタル双方向通信端末における暗号化・複号化装置においては、デジタル双方向通信端末に暗号化機能をダウンロードすることによって暗号化・復号化機能を実現させることが可能となるばかりでなく、データと同様にアプリケーションをダウンロードすることが可能であり、更にダウンロードされたアプリケーションをダイナミックに動作可能とするＯＳ／９の特徴を利用した暗号化・複号化機能が実現できる。

【００１７】また、認証機能のＨ／Ｗによる実装を行い、ユーザの認証を行うことによって、データの改ざん、不正なユーザによるなりすましを防ぐことができる。

【００１８】また、認証機能のＳ／Ｗによる実装を行うことによって、ユーザの認証を実現し、データの改ざんや不正ユーザによるなりすましを防ぐことができる。

【００１９】また、特にセキュリティの確保を必要とするデータを選択的に暗号化・複号化する機能を付加することよって、暗号化を必要としないデータをそのまま送受信することが可能となる。

【００２０】また、データが暗号化・複号化を必要とするか否かをサーバ側で決定し、そのリストをデジタル双方向通信端末にダウンロードしてサーバ側と端末側で共通のリストによって、暗号化・複号化を選択的に実行する機能を有することによって、ユーザの操作が不要となり、ユーザの操作の煩雑さをなくすと共に、ユーザによる誤操作の危険性を回避でき、さらに暗号化・復号化は共通なリストによって選択するため、データが暗号化されたものであるかどうかを示すフラグを送受信されるデータに付加する必要がなくなる。

【００２１】また、同じデータを何度も暗号化する必要がなくなり、デジタル双方向通信端末の負荷を軽減できる。

【００２２】以下、本発明をその実施の形態を示す図面に基づいて説明する。

実施の形態１．図１は本発明の実施の形態１であるを示すブロック図である。本実施の形態１において、ネットワークインターフェースモジュールはＡＤＳＬ対応であり、電話回線６に接続される。１から５の各モジュールは従来例で示したものと同様であり、その機能も図４０を用いて説明した従来ものと同様である。ただし、図１では、ＣＰＵモジュール２の不揮発性ＲＡＭ８にダウンロードされる暗号化モジュールが格納される。

【００２３】次に、本実施例におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。図２は実施例１における電源ＯＮ時のデジタル双方向通信端末の動作フローチャートである。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、Ｋｅｒｎｅｌの立ち上げを実行する。Ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール６のダウンロードを行う。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納される。図５に電話回線を介したサーバとデジタル双方向通信端末の接続図を示し、ダウンロードを行う際の暗号化モジュールの流れを示す。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線３６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９００（登録商標）　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK APIを使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。

【００２４】暗号化モジュール６がダウンロードされ、不揮発性ＲＡＭ８に格納されると、次にデジタル双方向通信端末は暗号化モジュール６の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムＲＯＭ１０のアプリケーション領域３０に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域３１に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末

は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【００２５】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。図３は実施の形態１におけるデータダウンロード時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作を示す。入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、ネットワークモジュール５へダウンロード命令とダウンロードすべきデータ名を受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図５に示した場合と同様にサーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線３６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。

【００２６】ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【００２７】図４は実施の形態１におけるデータ送信時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を示す。まず、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、電話回線を経由して、サーバに送信される。データの送信は図５に示す様に、ＯＳ－９０／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、電話回線３６に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６からデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に、復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。　以上の動作により、デジタル双方向通信端末はサ

ーバへデータを安全に送信することが可能となる。

【００２８】実施の形態２．本実施の形態２において、ネットワークインターフェースモジュールはＨＦＣ対応である。図６はネットワークインターフェースモジュールとしてＨＦＣを使用する場合のブロック図、図７はサーバとデジタル双方向通信端末の接続図である。図７および図４に示すように、デジタル双方向通信端末はネットワークインタフェースモジュールから同軸ケーブル４４、ファイバーバックボーン４２を経由してサービスプロバイダのサービス提供装置であるサーバに接続される。

【００２９】次に、本実施の形態２におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態２における電源ＯＮ時のデジタル双方向通信端末の動作フローチャートは図２と同様である。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、Ｋｅｒｎｅｌの立ち上げを実行する。Ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール６のダウンロードを行う。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納される。図７にダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れを示す。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２を通って、ファイバーと同軸ケーブルを接続するファイバーバックボーン４３を経由し、同軸ケーブル４４に接続されているデジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル４４に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。

【００３０】暗号化モジュール６がダウンロードされ、不揮発性ＲＡＭ８に格納されると、次にデジタル双方向通信端末は暗号化モジュール６の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムＲＯＭ１０のアプリケーション領域３０に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域３１に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【００３１】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。実施の形態２における暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作は図３と同様である。入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、ネットワークモジュール５へダウンロード命令とダウンロードすべきデータ名を受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図７に示したサーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２へ送信され、さらにファイバーバックボーン４３を経由し、同軸ケーブル４４を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル４４に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。

【００３２】ダウンロードされたデータはＣＰＵモジュ

ール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【００３３】実施の形態２における暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作は図４と同様である。まず、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、同軸ケーブル４４から送信され、ファイバーバックボーン４３、ファイバーケーブル４４を経由して、サーバに送信される。データの送信は図７に示す様に、ＯＳ－９／ＯＳ￥９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、同軸ケーブル４４に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２よりデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となる。

【００３４】実施の形態３．本実施の形態３において、ネットワークインターフェースモジュールはＡＴＭ対応である。図８はネットワークインターフェースモジュールとしてＡＴＭを使用する場合のブロック図、図９はＡＴＭネットワークを介して接続されるサーバとデジタル双方向通信端末間のデータの流れを示す図である。デジタル双方向通信端末はネットワークインタフェースモジュールからファイバーケーブル４６を経由し、ＡＴＭスイッチ４５を介してサービスプロバイダのサービス提供装置であるサーバに接続される。

【００３５】次に、本実施の形態３におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態３における電源ＯＮ時のデジタル双方向通信端末の動作フローチャートは図２と同様である。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、Ｋｅｒｎｅｌの立ち上げを実行する。Ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール６のダウンロードを行う。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納される。図９にダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れを示す。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２を通って、ＡＴＭスイッチ４５を経由し、ファイバーケーブル４６に接続されているデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル４６に接続されているハードウ

ェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。

【００３６】暗号化モジュール６がダウンロードされ、不揮発性ＲＡＭ８に格納されると、次にデジタル双方向通信端末は暗号化モジュール６の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムＲＯＭ１０のアプリケーション領域３０に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域３１に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【００３７】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。実施の形態３における暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作は図３と同様である。入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、ネットワークモジュールう５へダウンロード命令とダウンロードすべきデータ名を受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２へ送信され、さらにＡＴＭスイッチ４５を経由し、デジタル双方向通信端末に接続されたファイバーケーブル４６よりデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル４６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。

【００３８】ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【００３９】暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作は図４と同様である。まず、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用

暗号化鍵は、バスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、ＡＴＭ９送信される。データの送信は図９に示す様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、ファイバーケーブル４６に接続されているハードウェア３７から送信され、ＡＴＭスイッチを経由してサーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２よりデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。　以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となる。

【００４０】実施の形態４．図１０は本発明の実施の形態４であるシステム構成のブロック図である。本実施の形態において、ネットワークインターフェースモジュールはＡＤＳＬ対応であり、電話回線６に接続される。請求項２に記載されるデジタル双方向通信端末は認証・鍵配送のための暗号化モジュール（以下、Ｈ／Ｗ認証モジュール）をＨ／Ｗとして有しており、認識および鍵配送の暗号化処理にはＨ／Ｗ認証モジュールを使用する。

【００４１】次に、本実施の形態の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。図１１は実施の形態１における電源ＯＮ時のデジタル双方向通信端末の動作フローチャートである。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、ｋｅｒｎｅｌの立ち上げを実行する。ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末のＨ／Ｗ認証モジュールによって、デジタル双方向通信端末固有のＩＤ、ユーザのアクセスＩＤ、ユーザ名などの自分自身のデータを処理し、サーバへの暗号化モジュール要求に認証データと、認証に使用するためのデジタル双方向通信端末の公開鍵を付加してサーバへ送信し、暗号化モジュール６のダウンロードを要求する。サーバはデジタル双方向通信端末の公開鍵を使用して、デジタル双方向通信端末のデータを復号し、アクセス内容に改ざん、なりすましがないことを確認し、デジタル双方向通信端末からの暗号化モジュールのダウンロード要求を受け付ける。更にサーバは送信されたデジタル双方向通信端末の公開鍵を登録する。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図５と同様である。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線３６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。次にサーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンク、サーバによるデジタル双方向通信端末の認証、さらにサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【００４２】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。図１２はデータダウンロード時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作を示す。入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、Ｈ／Ｗ認証モジュールへダウンロード実行要求とダウンロードすべきデータ名をＨ／Ｗ認証モジュール１０へ受け渡す。ダウンロード実行要求とダウンロードすべきデータ名を受け取ったＨ／Ｗ認証モジュール１０は、認証のための暗号化を施し、ネットワークモジュール５へ暗号化されたダウンロード実行要求とダウンロードすべきデータ名を受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密

鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図５に示した場合と同様にサーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線３６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。

【００４３】ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。　以上の動作により、サーバはデジタル双方向通信端末からの要求に改ざんやなりすましのないことを確認することが可能となり、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【００４４】図１３はデータ送信時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を示す。まず、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してＨ／Ｗ認証モジュール１０へ受け渡される。暗号化されたデータとデータ用暗号化鍵を受け取ったＨ／Ｗ認証モジュール１０は、認証のための暗号化を施し、ネットワークモジュール５へ送信する。送信された認証のための暗号化を施されたデータはネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、電話回線を経由して、サーバに送信される。データの送信は図５に示す様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、電話回線３６に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６からデジタル双方向通信端末から送信されたデータを受信する。認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まずデジタル双方向通信端末の公開鍵を使用してデータの復号を行う。さらにサーバの秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またサーバは送信されたデータに改ざん、なりすましがないことを確認することが可能となる。

【００４５】実施の形態５．本発明の実施の形態３において、ネットワークインターフェースモジュールをＨＦＣ対応とすることができる。図１４は本発明の実施の形態５であるシステム構成を示すブロック図であり、ネットワークインターフェースモジュールとしてＨＦＣを使用する場合を示す。デジタル双方向通信端末はネットワークインタフェースモジュールから同軸ケーブルからファイバーバックボーンを経由してサービスプロバイダのサービス提供装置であるサーバに接続される。

【００４６】次に、本実施の形態３の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態５における電源ＯＮ時のデジタル双

方向通信端末の動作フローチャートは図１１と同様である。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、ｋｅｒｎｅｌの立ち上げを実行する。ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末のＨ／Ｗ認証モジュールによって、デジタル双方向通信端末固有のＩＤ、ユーザのアクセスＩＤ、ユーザ名などの自分自身のデータを処理し、サーバへの暗号化モジュール要求に認証データと、認証に使用するためのデジタル双方向通信端末の公開鍵を付加してサーバへ送信し、暗号化モジュール６のダウンロードを要求する。サーバはデジタル双方向通信端末の公開鍵を使用して、デジタル双方向通信端末のデータを復号し、アクセス内容に改ざん、なりすましがないことを確認し、デジタル双方向通信端末からの暗号化モジュールのダウンロード要求を受け付ける。更にサーバは送信されたデジタル双方向通信端末の公開鍵を登録する。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図７と同様である。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からファイバーバックボーン４３を経由し、同軸ケーブル４４に接続されたデジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル４４に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。次にサーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンク、サーバによるデジタル双方向通信端末の認証、さらにサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【００４７】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図１２と同様である。入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、Ｈ／Ｗ認証モジュールへダウンロード実行要求とダウンロードすべきデータ名をＨ／Ｗ認証モジュール１０へ受け渡す。ダウンロード実行要求とダウンロードすべきデータ名を受け取ったＨ／Ｗ認証モジュール１０は、認証のための暗号化を施し、ネットワークモジュールう５へ暗号化されたダウンロード実行要求とダウンロードすべきデータ名を受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図７に示した場合と同様にサーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からファイバーバックボーン４３を経由して同軸ケーブル４４に接続されたデジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル４４に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。

【００４８】ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デ

マルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、サーバはデジタル双方向通信端末からの要求に改ざんやなりすましのないことを確認することが可能となり、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【００４９】暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作のフローチャートは図１３と同様である。まず、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してＨ／Ｗ認証モジュール１０へ受け渡される。暗号化されたデータとデータ用暗号化鍵を受け取ったＨ／Ｗ認証モジュール１０は、認証のための暗号化を施し、ネットワークモジュール５へ送信する。送信された認証のための暗号化を施されたデータはネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、ＨＦＣ８を経由して、サーバに送信される。データの送信は図１１に示す様に、ＯＳ－９／ＯＳ－９００００３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、ファイバーケーブル４２に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からファイバーバックボーン４３を経由し、同軸ケーブルからデジタル双方向通信端末が送信した認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵をを受信する。認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まずデジタル双方向通信端末の公開鍵を使用してデータの復号を行う。さらにサーバの秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またサーバは送信されたデータに改ざん、なりすましがないことを確認することが可能となる。

【００５０】実施の形態６．本発明の実施の形態３において、ネットワークインターフェースモジュールをＡＴＭ対応とすることができる。図１５は本発明の実施の形態６であるシステム構成を示すブロック図であり、ネットワークインターフェースモジュールとしてＡＴＭを使用する場合を示す。デジタル双方向通信端末はネットワークインタフェースモジュールからＡＴＭを経由してサービスプロバイダのサービス提供装置であるサーバに接続される。

【００５１】次に、本実施の形態６の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態６における電源ＯＮ時のデジタル双方向通信端末の動作フローチャートは図１１と同様である。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、ｋｅｒｎｅｌの立ち上げを実行する。ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末のＨ／Ｗ認証モジュールによって、デジタル双方向通信端末固有のＩＤ、ユーザのアクセスＩＤ、ユーザ名などの自分自身のデータを処理し、サーバへの暗号化モジュール要求に認証データと、認証に使用するためのデジタル双方向通信端末の公開鍵を付加してサーバへ送信し、暗号化モジュール６のダウンロードを要求する。サーバはデジタル双方向通信端末の公開鍵を使用して、デジタル双方向通信端末のデータを復号し、アクセス内容に改ざん、なりすましがないことを確認し、デジタル双方向通信端末からの暗号化モジュールのダウンロード要求を受け付ける。更にサーバは送信されたデジタル双方向通信端末の公開鍵を登録する。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図９と同様である。サーバのアプリケーショ

ン領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からＡＴＭスイッチ４５を経由し、ファイバーケーブル４６に接続されたデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル４６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。次にサーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンク、サーバによるデジタル双方向通信端末の認証、さらにサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【００５２】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図１２と同様である。入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、Ｈ／Ｗ認証モジュールへダウンロード実行要求とダウンロードすべきデータ名をＨ／Ｗ認証モジュール１０へ受け渡す。ダウンロード実行要求とダウンロードすべきデータ名を受け取ったＨ／Ｗ認証モジュール１０は、認証のための暗号化を施し、ネットワークモジュールう５へ暗号化されたダウンロード実行要求とダウンロードすべきデータ名を受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図９に示した場合と同様にサーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からＡＴＭスイッチ４５を経由してファイバーケーブル４６に接続されたデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル４６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９００３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。

【００５３】ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、サーバはデジタル双方向通信端末からの要求に改ざんやなりすましのないことを確認することが可能となり、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【００５４】次に実施の形態６において、暗号化を施されたデータを送信する場合を説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図１３と同様である。まず、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジ

ュール６を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してＨ／Ｗ認証モジュール１０へ受け渡される。暗号化されたデータとデータ用暗号化鍵を受け取ったＨ／Ｗ認証モジュール１０は、認証のための暗号化を施し、ネットワークモジュール５へ送信する。送信された認証のための暗号化を施されたデータはネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、ＡＴＭ９を経由して、サーバに送信される。データの送信は図９と同様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、ファイバーケーブル４２に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からＡＴＭスイッチ４５を経由し、ファイバーケーブル４６からデジタル双方向通信端末が送信した認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵をを受信する。認証のための暗号化を施され、さらに暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まずデジタル双方向通信端末の公開鍵を使用してデータの復号を行う。さらに、サーバの秘密鍵を使用してデータ用暗号化鍵を復号する。次に、復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またサーバは送信されたデータに改ざん、なりすましがないことを確認することが可能となる。

【００５５】実施の形態７．図１６は本発明の実施の形態７であるシステム構成を示すブロック図である。本実施の形態７において、ネットワークインターフェースモジュールはＡＤＳＬ対応であり、電話回線６に接続される。請求項２に記載されるデジタル双方向通信端末は認証・鍵配送のための暗号化モジュール（以下、Ｓ／Ｗ認証モジュール）をＳ／Ｗとして有しており、認識および鍵配送の暗号化処理にはＳ／Ｗ認証モジュールを使用する。Ｓ／Ｗ認証モジュールはシステムＲＯＭのアプリケーション領域に組み込まれる。

【００５６】次に、本実施の形態７の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施例７における電源ＯＮ時のデジタル双方向通信端末の動作フローチャートは図１１と同様である。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、ｋｅｒｎｅｌの立ち上げを実行する。ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末のＳ／Ｗ認証モジュールによって、デジタル双方向通信端末固有のＩＤ、ユーザのアクセスＩＤ、ユーザ名などの自分自身のデータを処理し、サーバへの暗号化モジュール要求に認証データと、認証に使用するためのデジタル双方向通信端末の公開鍵を付加してサーバへ送信し、暗号化モジュール６のダウンロードを要求する。サーバはデジタル双方向通信端末の公開鍵を使用して、デジタル双方向通信端末のデータを復号し、アクセス内容に改ざん、なりすましがないことを確認し、デジタル双方向通信端末からの暗号化モジュールのダウンロード要求を受け付ける。更にサーバは送信されたデジタル双方向通信端末の公開鍵を登録する。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図５と同様である。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線３６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。次にサーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンク、サーバによるデジタル双方向通信端末の認証、さらにサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【００５７】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信に

ついて説明する。実施例７において暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作は図１２と同様である。入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、Ｓ／Ｗ認証モジュールへダウンロード実行要求とダウンロードすべきデータ名をＳ／Ｗ認証モジュール１１へ受け渡す。ダウンロード実行要求とダウンロードすべきデータ名を受け取ったＳ／Ｗ認証モジュール１１は、認証のための暗号化を施し、ネットワークモジュールう５へ暗号化されたダウンロード実行要求とダウンロードすべきデータ名を受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図５に示した場合と同様にサーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線３６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。

【００５８】ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、サーバはデジタル双方向通信端末からの要求に改ざんやなりすましのないことを確認することが可能となり、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【００５９】実施の形態７において、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作は図１３と同様である。まず、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してＳ／Ｗ認証モジュール１１へ受け渡される。暗号化されたデータとデータ用暗号化鍵を受け取ったＳ／Ｗ認証モジュール１１は、認証のための暗号化を施し、ネットワークモジュール５へ送信する。送信された認証のための暗号化を施されたデータはネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、電話回線を経由して、サーバに送信される。データの送信は図５に示す様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、電話回線３６に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６からデジタル双方向通信端末から送信されたデータを受信する。認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まずデジタル双方向通信端末の公開鍵を使用してデータの復号を行う。さらに、サーバの秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化

鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またサーバは送信されたデータに改ざん、なりすましがないことを確認することが可能となる。

【００６０】実施の形態８．本発明の実施の形態３において、ネットワークインターフェースモジュールをＨＦＣ対応とすることができる。図１７は実施の形態８であるシステム構成を示すブロック図であり、ネットワークインタフェースモジュールとしてＨＦＣを使用する場合を示す。デジタル双方向通信端末はネットワークインタフェースモジュールから同軸ケーブルからファイバーバックボーンを経由してサービスプロバイダのサービス提供装置であるサーバに接続される。

【００６１】次に、本実施の形態８の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態８における電源ＯＮ時のデジタル双方向通信端末の動作フローチャートは図１１と同様である。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、ｋｅｒｎｅｌの立ち上げを実行する。ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末のＳ／Ｗ認証モジュールによって、デジタル双方向通信端末固有のＩＤ、ユーザのアクセスＩＤ、ユーザ名などの自分自身のデータを処理し、サーバへの暗号化モジュール要求に認証データと、認証に使用するためのデジタル双方向通信端末の公開鍵を付加してサーバへ送信し、暗号化モジュール６のダウンロードを要求する。サーバはデジタル双方向通信端末の公開鍵を使用して、デジタル双方向通信端末のデータを復号し、アクセス内容に改ざん、なりすましがないことを確認し、デジタル双方向通信端末からの暗号化モジュールのダウンロード要求を受け付ける。更にサーバは送信されたデジタル双方向通信端末の公開鍵を登録する。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図７と同様である。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からファイバーバックボーン４３を経由し、同軸ケーブル４４に接続されたデジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル４４に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。次に、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンク、サーバによるデジタル双方向通信端末の認証、さらにサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【００６２】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。実施の形態８において暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図１２と同様である。入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、Ｓ／Ｗ認証モジュールへダウンロード実行要求とダウンロードすべきデータ名をＳ／Ｗ認証モジュール１１へ受け渡す。ダウンロード実行要求とダウンロードすべきデータ名を受け取ったＳ／Ｗ認証モジュール１１は、認証のための暗号化を施し、ネットワークモジュールう５へ暗号化されたダウンロード実行要求とダウンロードすべきデータ名を受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図７に示した場合と同様にサーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からファイバーバックボーン４３を経

由して同軸ケーブル４４に接続されたデジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル４４に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。

【００６３】ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、サーバはデジタル双方向通信端末からの要求に改ざんやなりすましのないことを確認することが可能となり、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【００６４】実施の形態８における暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図１３と同様である。まず、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してＳ／Ｗ認証モジュール１１へ受け渡される。暗号化されたデータとデータ用暗号化鍵を受け取ったＳ／Ｗ認証モジュール１１は、認証のための暗号化を施し、ネットワークモジュール５へ送信する。送信された認証のための暗号化を施されたデータはネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、ＨＦＣ８を経由して、サーバに送信される。データの送信は図７に示す様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、ファイバーケーブル４２に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からファイバーバックボーン４３を経由し、同軸ケーブルからデジタル双方向通信端末が送信した認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵ををを受信する。認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まずデジタル双方向通信端末の公開鍵を使用してデータの復号を行う。さらにサーバの秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またサーバは送信されたデータに改ざん、なりすましがないことを確認することが可能となる。

【００６５】実施の形態９．本発明の実施の形態７において、ネットワークインターフェースモジュールをＡＴＭ対応とすることができる。図１８は実施の形態９であるシステム構成を示すブロック図であり、ネットワークインターフェースモジュールとしてＡＴＭを使用する場合を示す。デジタル双方向通信端末はネットワークインタフェースモジュールからＡＴＭを経由してサービスプロバイダのサービス提供装置であるサーバに接続される。

【００６６】次に、本実施の形態９の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態９における電源ＯＮ時のデジタル双方向通信端末の動作フローチャートは図１１と同様である。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、

システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、ｋｅｒｎｅｌの立ち上げを実行する。ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末のＳ／Ｗ認証モジュールによって、デジタル双方向通信端末固有のＩＤ、ユーザのアクセスＩＤ、ユーザ名などの自分自身のデータを処理し、サーバへの暗号化モジュール要求に認証データと、認証に使用するためのデジタル双方向通信端末の公開鍵を付加してサーバへ送信し、暗号化モジュール６のダウンロードを要求する。サーバはデジタル双方向通信端末の公開鍵を使用して、デジタル双方向通信端末のデータを復号し、アクセス内容に改ざん、なりすましがないことを確認し、デジタル双方向通信端末からの暗号化モジュールのダウンロード要求を受け付ける。更にサーバは送信されたデジタル双方向通信端末の公開鍵を登録する。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図９と同様である。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からＡＴＭスイッチ４５を経由し、ファイバーケーブル４６に接続されたデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル４６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。次にサーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンク、サーバによるデジタル双方向通信端末の認証、さらにサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【００６７】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図１２と同様である。入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、Ｓ／Ｗ認証モジュールへダウンロード実行要求とダウンロードすべきデータ名をＳ／Ｗ認証モジュール１１へ受け渡す。ダウンロード実行要求とダウンロードすべきデータ名を受け取ったＳ／Ｗ認証モジュール１１は、認証のための暗号化を施し、ネットワークモジュールう５へ暗号化されたダウンロード実行要求とダウンロードすべきデータ名を受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図９に示した場合と同様にサーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からＡＴＭスイッチ４５を経由してファイバーケーブル４６に接続されたデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル４６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。

【００６８】ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイ

コントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、サーバはデジタル双方向通信端末からの要求に改ざんやなりすましのないことを確認することが可能となり、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【００６９】暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図１３と同様である。まず、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してＳ／Ｗ認証モジュール１１へ受け渡される。暗号化されたデータとデータ用暗号化鍵を受け取ったＳ／Ｗ認証モジュール１１は、認証のための暗号化を施し、ネットワークモジュール５へ送信する。送信された認証のための暗号化を施されたデータはネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、ＨＦＣ８を経由して、サーバに送信される。データの送信は図９に示す様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、ファイバーケーブル４２に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からＡＴＭスイッチ４５を経由し、ファイバーケーブル４６からデジタル双方向通信端末が送信した認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵ををを受信する。認証のための暗号化を施され、更に暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まずデジタル双方向通信端末の公開鍵を使用してデータの復号を行う。さらにサーバの秘密鍵を使用してデータ用暗号化鍵を復号する。次に、復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またサーバは送信されたデータに改ざん、なりすましがないことを確認することが可能となる。

【００７０】実施の形態１０．図１９は本発明の実施の形態１０であるシステム構成を示すブロック図である。本実施の形態において、ネットワークインターフェースモジュールはＡＤＳＬ対応であり、電話回線６に接続される。

【００７１】次に、本実施の形態１０であるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態１０における電源ＯＮ時のデジタル双方向通信端末の動作フローチャートを図２０に示す。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、ｋｅｒｎｅｌの立ち上げを実行する。ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール６のダウンロードを行う。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納される。図５にダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れを示す。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線３６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。

【００７２】暗号化モジュール６がダウンロードされ、不揮発性ＲＡＭ８に格納されると、次にデジタル双方向通信端末は暗号化モジュール６の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムＲＯＭ１０のアプリケーション領域３０に保存されている。サーバはデジタル双方向通信端末から送信

されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域３１に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【００７３】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。図２１はデータダウンロード時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作を示す。デジタル双方向通信端末は入力モジュール１からユーザによって入力された暗号化ＯＮ／ＯＦＦ命令受信し、バスを通じてシステムＲＡＭ９に暗号化ＯＮ／ＯＦＦのフラグ（データ暗号化フラグ）を記憶する。本実施の形態１０における暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作は、サーバへの要求にデータ暗号化フラグを添付すること以外は図２と同様である。入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、ネットワークモジュール５へダウンロード命令とダウンロードすべきデータ名とデータ暗号化フラグを受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名とデータ暗号化フラグをサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側ではデータ暗号化フラグによって示されるデータ暗号化のＯＮ／ＯＦＦを確認し、データ暗号化がＯＮであるこ場合、秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データの暗号化がＯＦＦである場合、サーバはデータの暗号化を施さず、要求されたデータを送信する。

【００７４】データのダウンロードは図５に示した場合と同様にUPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線３６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。データ暗号化がＯＮである場合、ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。データ暗号化がＯＦＦの場合は、復号化は省略される。受信されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【００７５】図２２はデータ送信時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を示す。まず、デジタル双方向通信端末はシステムＲＡＭに記憶されたデータ暗号化フラグをチェックし、データ暗号化フラグがＯＮである場合、送信しようとするデータの暗号化を実行する。データ暗号化フラグがＯＮである場合、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用し

たデータ用暗号化鍵は暗号化モジュール６を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、電話回線を経由して、サーバに送信される。データの送信は図５に示す様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、電話回線３６に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６からデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。

【００７６】データ暗号化フラグがＯＦＦである場合、サーバに送信すべきデータはバスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、電話回線を経由して、サーバに送信される。データの送信は図５に示す様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、電話回線３６に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６からデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【００７７】実施の形態１１．本実施の形態１１において、ネットワークインターフェースモジュールはＨＦＣ対応である。図２３は実施の形態１１であるシステム構成を示すブロック図であり、ネットワークインターフェースモジュールとしてＨＦＣを使用する場合を示す。デジタル双方向通信端末はネットワークインタフェースモジュールから同軸ケーブルからファイバーバックボーンを経由してサービスプロバイダのサービス提供装置であるサーバに接続される。

【００７８】次に、本実施の形態１１におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態１１における電源ＯＮ時のデジタル双方向通信端末の動作フローチャートは図２０と同様である。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、ｋｅｒｎｅｌの立ち上げを実行する。ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール６のダウンロードを行う。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納される。図７にダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れを示す。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からファイバーバックボーン４３を経由して同軸ケーブル４４からデジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル４４に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＡ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。

【００７９】暗号化モジュール６がダウンロードされ、不揮発性ＲＡＭ８に格納されると、次にデジタル双方向通信端末は暗号化モジュール６の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムＲＯＭ１０のアプリケーション領域３０に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域３１に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存す

る。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【００８０】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図２１と同様である。デジタル双方向通信端末は入力モジュール１からユーザによって入力された暗号化ＯＮ／ＯＦＦ命令受信し、バスを通じてシステムＲＡＭ９に暗号化ＯＮ／ＯＦＦのフラグ（データ暗号化フラグ）を記憶する。本実施の形態１１における暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作は、サーバへの要求にデータ暗号化フラグを添付すること以外は図６と同様である。入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、ネットワークモジュール５へダウンロード命令とダウンロードすべきデータ名とデータ暗号化フラグを受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名とデータ暗号化フラグをサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側ではデータ暗号化フラグによって示されるデータ暗号化のＯＮ／ＯＦＦを確認し、データ暗号化がＯＮであるこ場合、秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データの暗号化がＯＦＦである場合、サーバはデータの暗号化を施さず、要求されたデータを送信する。

【００８１】データのダウンロードは図７に示した場合と同様にUPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からファイバーバックボーン４３を経由して同軸ケーブル４４からデジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル４４に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。データ暗号化がＯＮである場合、ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。データ暗号化がＯＦＦの場合は、復号化は省略される。受信されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【００８２】次に暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図２２と同様である。まず、デジタル双方向通信端末はシステムＲＡＭに記憶されたデータ暗号化フラグをチェックし、データ暗号化フラグがＯＮである場合、送信しようとするデータの暗号化を実行する。データ暗号化フラグがＯＮである場合、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサ

ーバの公開鍵を用いて暗号化する。次に、デジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、同軸ケーブル４４からファイバーバックボーン４３、ファイバーケーブル４２を経由して、サーバに送信される。データの送信は図７に示す様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、ファイバーケーブル４２に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている同軸ケーブル４４を使用してデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に、復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。

【００８３】データ暗号化フラグがＯＦＦである場合、サーバに送信すべきデータはバスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、同軸ケーブル４４からファイバーバックボーン４３、ファイバーケーブル４２を経由して、サーバに送信される。データの送信は図７に示す様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、ファイバーケーブル４２に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている同軸ケーブル４４からファイバーバックボーン４３、ファイバーケーブル４２を経由してデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【００８４】実施の形態１２．本実施の形態１２において、ネットワークインターフェースモジュールはＡＴＭ対応である。図２４は実施の形態１２であるシステム構成を示すブロック図であり、ネットワークインターフェースモジュールとしてＡＴＭを使用する場合を示す。デジタル双方向通信端末はネットワークインタフェースモジュールから光ファイバーケーブルを経由し、ＡＴＭスイッチを介してサービスプロバイダのサービス提供装置であるサーバに接続される。

【００８５】次に、本実施の形態１２におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施例１２における電源ＯＮ時のデジタル双方向通信端末の動作フローチャートは図２０と同様である。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、ｋｅｒｎｅｌの立ち上げを実行する。ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール６のダウンロードを行う。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図９と同様である。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からＡＴＭスイッチ４５を経由して、ファイバーケーブル４６からデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル４６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。

【００８６】暗号化モジュール６がダウンロードされ、不揮発性ＲＡＭ８に格納されると、次にデジタル双方向通信端末は暗号化モジュール６の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムＲＯＭ１０のアプリケーション領域３０に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信

したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域３１に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【００８７】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図２１と同様である。デジタル双方向通信端末は入力モジュール１からユーザによって入力された暗号化ＯＮＮ／ＯＦＦ命令受信し、バスを通じてシステムＲＡＭ９に暗号化ＯＮ／ＯＦＦのフラグ（データ暗号化フラグ）を記憶する。入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、ネットワークモジュールう５へダウンロード命令とダウンロードすべきデータ名とデータ暗号化フラグを受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名とデータ暗号化フラグをサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側ではデータ暗号化フラグによって示されるデータ暗号化のＯＮ／ＯＦＦを確認し、データ暗号化がＯＮであるこ場合、秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データの暗号化がＯＦＦである場合、サーバはデータの暗号化を施さず、要求されたデータを送信する。

【００８８】データのダウンロードは図９に示した場合と同様にUPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からＡＴＭスイッチ４５からファイバーケーブル４６を経由してデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル４６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。データ暗号化がＯＮである場合、ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。データ暗号化がＯＦＦの場合は、復号化は省略される。受信されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【００８９】次に暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を示す。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図２２と同様である。まず、デジタル双方向通信端末はシステムＲＡＭに記憶されたデータ暗号化フラグをチェックし、データ暗号化フラグがＯＮである場合、送信しようとするデータの暗号化を実行する。データ暗号化フラグがＯＮである場合、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサーバ

の公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、ファイバーケーブル４６からＡＴＭスイッチ４５、ファイバーケーブル４２を経由して、サーバに送信される。データの送信は図９に示すのと同様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、ファイバーケーブル４２に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４６を使用してデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。

【００９０】データ暗号化フラグがＯＦＦである場合、サーバに送信すべきデータはバスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、ファイバーケーブル４６からＡＴＭスイッチ４５、ファイバーケーブル４２を経由して、サーバに送信される。データの送信は図９に示す様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、ファイバーケーブル４２に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４６、ＡＴＭスイッチ４５、ファイバーケーブル４２を経由してデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【００９１】実施の形態１３．図２５は本発明の実施の形態１３であるシステム構成を示すブロック図である。本実施の形態１３において、ネットワークインターフェースモジュールはＡＤＳＬ対応であり、電話回線６に接続される。

【００９２】次に、本実施の形態１３におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態１０における電源ＯＮ時のデジタル双方向通信端末の動作フローチャートを図２６に示す。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、ｋｅｒｎｅｌの立ち上げを実行する。ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール６と暗号化を行うべきデータのリストである暗号化適用データリスト１２のダウンロードを行う。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納され、暗号化適用データリストはシステムＲＡＭ１０に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図５と同様である。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線３６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、OS-9/OS-9000３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。

【００９３】暗号化モジュール６がダウンロードされ、不揮発性ＲＡＭ８に格納されると、次にデジタル双方向通信端末は暗号化モジュール６の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムＲＯＭ１０のアプリケーション領域３０に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域３１に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末

は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【００９４】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。図２７はダウンロード時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作を示す。デジタル双方向通信端末は入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、ネットワークモジュールう５へダウンロード命令とダウンロードすべきデータ名とデータ暗号化フラグを受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名とデータ暗号化フラグをサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では要求されたデータが暗号化適用データリストに含まれるかどうかを確認し、送信すべきデータが暗号化適用データリストに含まれる場合、秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。要求されたデータが暗号化適用データリストに含まれない場合、サーバはデータの暗号化を施さず、要求されたデータを送信する。

【００９５】データのダウンロードは図９に示した場合と同様にUPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線３６に接続されているハードウエア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。デジタル双方向通信端末は、暗号化適用データリスト１２を参照し、ダウンロードしたデータが暗号化適用データリストに含まれる場合、ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。データ暗号化がＯＦＦの場合は、復号化は省略される。受信されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【００９６】次に暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を説明する。図２８はデータ送信時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を示す。まず、デジタル双方向通信端末はシステムＲＡＭに記憶された暗号化適用データリスト１２を参照し、送信すべきデータが暗号化適用データリストに含まれる場合、送信しようとするデータの暗号化を実行する。データの暗号化を行う場合、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、電話回線を経

由して、サーバに送信される。データの送信は図５に示す様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、電話回線３６に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６からデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。

【００９７】送信すべきデータが暗号化適用データリストに含まれない場合、サーバに送信すべきデータはバスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、電話回線を経由して、サーバに送信される。データの送信は図５に示す様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、電話回線３６に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６からデジタル双方向通信端末から送信されたデータを受信する。データを受信したサーバはデータが暗号化適用データリスト１２に含まれないことを確認して、データはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【００９８】実施の形態１４．本実施の形態１４において、ネットワークインターフェースモジュールはＨＦＣ対応である。図２９は本発明の実施の形態１４であるシステム構成を示すブロック図であり、ネットワークインターフェースモジュールとしてＨＦＣを使用する場合を示す。デジタル双方向通信端末はネットワークインタフェースモジュールから同軸ケーブルからファイバーバックボーンを経由してサービスプロバイダのサービス提供装置であるサーバに接続される。

【００９９】次に、本実施の形態１４におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態１２における電源ＯＮ時のデジタル双方向通信端末の動作フローチャートは図２６と同様である。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、ｋｅｒｎｅｌの立ち上げを実行する。ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール６と暗号化を行うべきデータのリストである暗号化適用データリスト１２のダウンロードを行う。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納され、暗号化適用データリストはシステムＲＡＭ１０に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図９と同様である。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２、ファイバーバックボーン４３、同軸ケーブル４４を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル４６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK APＩを使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。

【０１００】暗号化モジュール６がダウンロードされ、不揮発性ＲＡＭ８に格納されると、次にデジタル双方向通信端末は暗号化モジュール６の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムＲＯＭ１０のアプリケーション領域３０に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域３１に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が

行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【０１０１】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図２９と同様である。デジタル双方向通信端末は入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、ネットワークモジュールう５へダウンロード命令とダウンロードすべきデータ名とデータ暗号化フラグを受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名とデータ暗号化フラグをサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では要求されたデータが暗号化適用データリストに含まれるかどうかを確認し、送信すべきデータが暗号化適用データリストに含まれる場合、秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。要求されたデータが暗号化適用データリストに含まれない場合、サーバはデータの暗号化を施さず、要求されたデータを送信する。データのダウンロードは図７に示した場合と同様にUPLINK/DOWNLINK APＩ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２、ファイバーバックボーン４３、同軸ケーブル４４を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル４６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。

【０１０２】デジタル双方向通信端末は、暗号化適用データリスト１２を参照し、ダウンロードしたデータが暗号化適用データリストに含まれる場合、ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。データ暗号化がＯＦＦの場合は、復号化は省略される。受信されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【０１０３】次に暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図２８と同様である。まず、デジタル双方向通信端末はシステムＲＡＭに記憶された暗号化適用データリスト１２を参照し、送信すべきデータが暗号化適用データリストに含まれる場合、送信しようとするデータの暗号化を実行する。データの暗号化を行う場合、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサーバの公開鍵を用いて暗号化する。次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、ファイバーケーブル４６からＡＴＭスイッチ４５、ファイバーケーブル４２を経由して、サーバに送信される。データの送信は図７に示す様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであ

るUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、ファイバーケーブル４２に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている同軸ケーブル４４からデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。

【０１０４】送信すべきデータが暗号化適用データリストに含まれない場合、サーバに送信すべきデータはバスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、ファイバーケーブル４６からＡＴＭスイッチ、ファイバーケーブル４２を経由して、サーバに送信される。データの送信は図９に示す様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、ファイバーケーブル４２に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からファイバーバックボーン４３、同軸ケーブル４４を経由してデジタル双方向通信端末から送信されたデータを受信する。データを受信したサーバはデータが暗号化適用データリスト１２に含まれないことを確認して、データはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【０１０５】実施の形態１５．本実施の形態１５において、ネットワークインターフェースモジュールはＡＴＭ対応である。図３０は実施の形態１５であるシステム構成を示すブロック図であり、ネットワークインターフェースモジュールとしてＡＴＭを使用する場合を示す。デジタル双方向通信端末はネットワークインタフェースモジュールから光ファイバーケーブルを経由し、ＡＴＭスイッチを介してサービスプロバイダのサービス提供装置であるサーバに接続される。

【０１０６】次に、本実施の形態１５におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施ＮＯ形態１５における電源ＯＮ時のデジタル双方向通信端末の動作フローチャートは図２６と同様である。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、ｋｅｒｎｅｌの立ち上げを実行する。ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール６のダウンロードを行う。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納される。図９にダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れを示している。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からＡＴＭスイッチ４５を経由して、ファイバーケーブル４６からデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル４６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。

【０１０７】暗号化モジュール６がダウンロードされ、不揮発性ＲＡＭ８に格納されると、次にデジタル双方向通信端末は暗号化モジュール６の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムＲＯＭ１０のアプリケーション領域３０に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域３１に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のように、デジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【０１０８】次に、実行可能となった暗号化モジュール

を使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図２９と同様である。デジタル双方向通信端末は入力モジュール１からユーザによって入力された暗号化ON/OFF命令受信し、バスを通じてシステムＲＡＭ９に暗号化ON/OFFのフラグ（データ暗号化フラグ）を記憶する。入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、ネットワークモジュールう５へダウンロード命令とダウンロードすべきデータ名とデータ暗号化フラグを受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名とデータ暗号化フラグをサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側ではデータ暗号化フラグによって示されるデータ暗号化のＯＮ／ＯＦＦを確認し、データ暗号化がＯＮである場合、秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データの暗号化がＯＦＦである場合、サーバはデータの暗号化を施さず、要求されたデータを送信する。データのダウンロードは図９に示した場合と同様にUPLINK/DOWNLINKAPI ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２からＡＴＭスイッチ４５からファイバーケーブル４６を経由してデジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル４６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。

【０１０９】データ暗号化がＯＮである場合、ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。データ暗号化がＯＦＦの場合は、復号化は省略される。受信されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【０１１０】次に暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図２８と同様である。まず、デジタル双方向通信端末はシステムＲＡＭに記憶されたデータ暗号化フラグをチェックし、データ暗号化フラグがＯＮである場合、送信しようとするデータの暗号化を実行する。データ暗号化フラグがＯＮである場合、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次に、デジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサーバの公開鍵を用いて暗号化する。次に、デジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、ファイバーケーブル４６からＡＴＭスイッチ４５、ファイバーケーブル４２を経由して、サーバに送信される。データの送信は図９に示した様に、ＯＳ－９／ＯＳ－９００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、ファイバーケーブル４２に接続されているハードウェア３

７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４６を使用してデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に、復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。

【０１１１】データ暗号化フラグがＯＦＦである場合、サーバに送信すべきデータはバスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、ファイバーケーブル４６からＡＴＭスイッチ４５、ファイバーケーブル４２を経由して、サーバに送信される。データの送信は図９に示した様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API４０ を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、ファイバーケーブル４２に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６からデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に、復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となり、データによって暗号化が不要なデータの暗号化は省略することが可能となり、常に暗号化を施す場合に比較して効率よくデータの送受信を行うことが可能となる。

【０１１２】実施の形態１６．図３１は実施の形態１６であるシステム構成のブロック図である。本実施の形態１６において、ネットワークインターフェースモジュールはＡＤＳＬ対応であり、電話回線６に接続される。また、システムＲＡＭ内に一度暗号化を施したデータを記憶しておくための領域（暗号化データ記憶領域１３）を有する。

【０１１３】次に、本実施の形態１６におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。図３２はデジタル双方向通信端末電源ＯＮ時のフローチャートである。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、ｋｅｒｎｅｌの立ち上げを実行する。ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール６のダウンロードを行う。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図５と同様である。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINKAPI ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線３６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、OS-9/OS-9000３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。

【０１１４】暗号化モジュール６がダウンロードされ、不揮発性ＲＡＭ８に格納されると、次にデジタル双方向通信端末は暗号化モジュール６の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムＲＯＭ１０のアプリケーション領域３０に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域３１に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【０１１５】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。図３３はデータダウンロード時のフローチャートであり、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作を示す。入力モジュール１より、データダウンロード実行信号を受信したデジ

タル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、ネットワークモジュールう５へダウンロード命令とダウンロードすべきデータ名を受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図５に示した場合と同様にサーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では電話回線３６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。

【０１１６】ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【０１１７】図３４はデータ送信時のフローチャートであり、詳しくは、暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を示す。まず、デジタル双方向通信端末はシステムＲＡＭ内の暗号化データ記憶領域１３に、送信すべきデータの暗号化されたデータの検索を行う。暗号化データ記憶領域１３に送信すべきデータが存在しない場合、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサーバの公開鍵を用いて暗号化する。デジタル双方向通信端末は暗号化を施したデータと暗号化に使用した暗号化鍵をシステムＲＡＭ１０上の暗号化データ記憶領域１３に格納する。暗号化データ記憶領域の要領を超える場合には、最終の参照日時が最も篩いものから順にデータを消去する。暗号化データ記憶領域１３に送信すべきデータが存在する場合、デジタル双方向通信端末はそのデータと暗号化鍵をサーバに送信する。

【０１１８】次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、電話回線を経由して、サーバに送信される。データの送信は図５に示した様に、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、電話回線３６に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINKAPI ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている電話回線３６からデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またデジタル双方向通信端末におけるデータの暗号化処理の必要回数を減らすことが可能となり、サーバへのデータ送

信の効率を上げることが可能となる。

【０１１９】実施の形態１７．図３５は実施の形態１７であるシステム構成を示すブロック図である。本実施の形態１７において、ネットワークインターフェースモジュールはＨＦＣ対応であり、デジタル双方向通信端末は同軸ケーブル７に接続される。また、システムＲＡＭ内に一度暗号化を施したデータを記憶しておくための領域（暗号化データ記憶領域１３）を有する。

【０１２０】次に、本実施の形態１７におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施の形態１７における電源ＯＮ時のデジタル双方向通信端末の動作フローチャートは図３２と同様である。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、ｋｅｒｎｅｌの立ち上げを実行する。ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール６のダウンロードを行う。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納される。ダウンロードを行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図７と同様である。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２、ファイバーバックボーン４３を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル４４に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。

【０１２１】暗号化モジュール６がダウンロードされ、不揮発性ＲＡＭ８に格納されると、次にデジタル双方向通信端末は暗号化モジュール６の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムＲＯＭ１０のアプリケーション領域３０に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、この受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域３１に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のように、デジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【０１２２】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図３３と同様である。入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、ネットワークモジュールう５へダウンロード命令とダウンロードすべきデータ名を受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図７に示した場合と同様にサーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２、ファイバーバックボーン４３を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル４４に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。

【０１２３】ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号

化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【０１２４】次に暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図３４と同様である。まず、デジタル双方向通信端末はシステムＲＡＭ内の暗号化データ記憶領域１３に、送信すべきデータの暗号化されたデータの検索を行う。暗号化データ記憶領域１３に送信すべきデータが存在しない場合、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次にデジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサーバの公開鍵を用いて暗号化する。デジタル双方向通信端末は暗号化を施したデータと暗号化に使用した暗号化鍵をシステムＲＡＭ１０上の暗号化データ記憶領域１３に格納する。暗号化データ記憶領域の要領を超える場合には、最終の参照日時が最も篩いものから順にデータを消去する。暗号化データ記憶領域１３に送信すべきデータが存在する場合、デジタル双方向通信端末はそのデータと暗号化鍵をサーバに送信する。

【０１２５】次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、同軸ケーブル４４、ファイバーバックボーン４３を経由して、サーバに送信される。データの送信は図７と同様に、ＯＳ－９／ＯＳ－９００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、ファイバーケーブル４２に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されている同軸ケーブル４４からファイバーバックボーン４３を経由してデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またデジタル双方向通信端末におけるデータの暗号化処理の必要回数を減らすことが可能となり、サーバへのデータ送信の効率を上げることが可能となる。

【０１２６】実施の形態１８．図３６は実施の形態１８であるシステム構成を示すブロック図である。本実施の形態１８において、ネットワークインターフェースモジュールはＡＴＭ対応であり、デジタル双方向通信端末はファイバーケーブルに接続される。また、システムＲＡＭ内に一度暗号化を施したデータを記憶しておくための領域（暗号化データ記憶領域１３）を有する。

【０１２７】次に、本実施の形態１８におけるデジタル双方向通信端末の動作を説明する。まず、電源投入時のデジタル双方向通信端末の動作を説明する。実施例１８における電源ＯＮ時のデジタル双方向通信端末の動作フローチャートは図３２と同様である。入力モジュール１より、電源入の信号を受信したデジタル双方向通信端末は赤外線リモコンレシーバ７で信号が電源ＯＮ信号であることを解析し、ＣＰＵへ電源ＯＮ信号を送信する。電源ＯＮ信号を受信したＣＰＵモジュールは、各モジュール[１－５]の初期化を行う。次に、各モジュールが正常に動作しているかどうかのチェックを行うパワーＯＮセルフテストを実行する。次に、システムＲＯＭ９とシステムＲＡＭ１０の初期化を行う。次に、ｋｅｒｎｅｌの立ち上げを実行する。ｋｅｒｎｅｌの立ち上げが終了したあと、次にデジタル双方向通信端末はサーバへアクセスを行い、暗号化モジュール６のダウンロードを行う。ダウンロードした暗号化モジュール６はアプリケーションとして不揮発性ＲＡＭ８に格納される。ダウンロード

を行う際のサーバとデジタル双方向通信端末の接続図と暗号化モジュールの流れは図９と同様である。サーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２、ＡＴＭスイッチ４５を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側では同軸ケーブル４４に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のアプリケーション領域４１に格納される。ここでいうデジタル双方向通信端末のアプリケーション領域４１は、不揮発性ＲＡＭ８である。

【０１２８】暗号化モジュール６がダウンロードされ、不揮発性ＲＡＭ８に格納されると、次にデジタル双方向通信端末は暗号化モジュール６の初期化、リンクを行い暗号化モジュールを実行可能状態にする。次に、デジタル双方向通信端末は自分自身の公開鍵をサーバへ送信する。デジタル双方向通信端末の公開鍵と秘密鍵のペアはシステムＲＯＭ１０のアプリケーション領域３０に保存されている。サーバはデジタル双方向通信端末から送信されたデジタル双方向通信端末の公開鍵を受信し、受信したデジタル双方向通信端末の公開鍵をサーバのアプリケーション領域３１に登録し、サーバの公開鍵をデジタル双方向通信端末に送信する。デジタル双方向通信端末は受信したサーバの公開鍵を不揮発性ＲＡＭ８に保存する。以上のようにデジタル双方向通信端末への暗号化モジュールのダウンロードと初期化・リンクが行われ、またサーバとデジタル双方向通信端末間の公開鍵の交換が行われ、暗号化モジュール６のダウンロードを実行するデジタル双方向通信端末の電源ＯＮ動作が終了する。

【０１２９】次に、実行可能となった暗号化モジュールを使用したデジタル双方向通信端末のデータの送受信について説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバから暗号化を施されたデータを受信する際の動作フローチャートは図３３と同様である。入力モジュール１より、データダウンロード実行信号を受信したデジタル双方向通信端末は、入力信号を解析し、ダウンロード実行命令と、ダウンロードすべきデータ名をＣＰＵモジュール２へ受け渡す。ダウンロード命令を受信したＣＰＵモジュールは、ネットワークモジュールう５へダウンロード命令とダウンロードすべきデータ名を受け渡す。ネットワークモジュール５は制御チャネルＩ／Ｆ１８を通じて、ダウンロード実行要求と、ダウンロードすべきデータ名をサーバへ送信し、デジタル双方向通信端末からサーバへデータの転送を要求する。サーバ側では秘密鍵暗号方式による暗号化鍵を生成し、データを暗号化し、暗号化に使用した暗号化鍵をデジタル双方向通信端末から受信した公開鍵によって暗号化し、暗号化されたデータと暗号化鍵をデジタル双方向通信端末に送信する。データのダウンロードは図１３に示した場合と同様にサーバのアプリケーション領域３１に格納されている暗号化モジュール６は、デジタル双方向通信端末からの要求を受けて、UPLINK/DOWNLINK API ３２を使用し、サーバ用のＯＳ３３を介して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４２、ＡＴＭスイッチ４５を経由し、デジタル双方向通信端末へ送られる。デジタル双方向通信端末側ではファイバーケーブル４６に接続されているハードウェア３７から、ファイル・マネージャ、ドライバ３８によって、ＯＳ－９／ＯＳ－９０００　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API を使用して、デジタル双方向通信端末のシステムＲＡＭ１０に格納される。

【０１３０】ダウンロードされたデータはＣＰＵモジュール２の暗号化モジュール６を使用して復号される。暗号化されたデータと暗号化鍵を受信したデジタル双方向通信端末は、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。復号されたデータ用暗号化鍵は、システムＲＡＭ１０に保存される。次に復号され、システムＲＡＭに保存されたデータ用暗号化鍵を使用して、データの復号を行う。復号されたデータのうち、ＭＰＥＧデータ以外のデータはバスを通じてグラフィックモジュール３へ送信され、ＭＰＥＧデータはバスを介してデマルチプレクサシンクコントロール１６へ受け渡される。デマルチプレクサシンクコントロール１６に受け渡されたＭＰＥＧデータは、画像データと音声データの切り分け処理が行われ、同期をとって、ＭＰＥＧモジュール４へ受け渡される。ＭＰＥＧモジュール４に受け取られた画像データはＭＰＥＧビデオプロセッサ１４で、音声データはＭＰＥＧオーディオプロセッサ１５でそれぞれ復号処理され、ＭＰＥＧビデオプロセッサ１４で復号されたビデオ信号は、グラフィックモジュール３のオーバレイコントローラ１３に受け渡され、ＭＰＥＧオーディオプロセッサ１５で復号されたオーディオデータはステレオオーディオ出力へ出力される。バスを通じてグラフィックモジュール３へ受け渡された静止画像データは静止画像プロセッサ１２で復号処理され、オーバレイコントローラ１３へ受け渡される。オーバレイコントローラ１３では、静止画像プロセッサ１２から受け取った静止画像データとＭＰＥＧビデオプロセッサ１４から受け取ったビデオデータの重ね合わせ処理を行い、ビデオ出力へ出力する。以上の動作により、デジタル双方向通信端末はサーバからのデータを安全に受信することが可能となる。

【０１３１】次に暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作を説明する。暗号化モジュールが実行可能状態となったデジタル双方向通信端末がサーバへ暗号化を施されたデータを送信する際の動作フローチャートは図３４と同様である。まず、デジタル双方向通信端末はシステムＲＡＭ内の暗号化データ記憶領域１３に、送信すべきデータの暗号化されたデータの検索を行う。暗号化データ記憶領域１３に送信すべきデータが存在しない場合、デジタル双方向通信端末はＣＰＵモジュール２において、暗号化モジュール６を用いて暗号化鍵を生成する。次に、デジタル双方向通信端末は暗号化モジュール６によってサーバに送信すべきデータの暗号化を行い、データの暗号化に使用したデータ用暗号化鍵は暗号化モジュール６を使用してサーバの公開鍵を用いて暗号化する。デジタル双方向通信端末は暗号化を施したデータと暗号化に使用した暗号化鍵をシステムＲＡＭ１０上の暗号化データ記憶領域１３に格納する。暗号化データ記憶領域の要領を超える場合には、最終の参照日時が最も篩いものから順にデータを消去する。暗号化データ記憶領域１３に送信すべきデータが存在する場合、デジタル双方向通信端末はそのデータと暗号化鍵をサーバに送信する。

【０１３２】次にデジタル双方向通信端末は暗号化されたデータとデータ用暗号化鍵は、バスを介してネットワークモジュール５の制御チャネルＩ／Ｆへ送られ、制御チャネルＩ／Ｆを介して、同軸ケーブル４４、ファイバーバックボーン４３を経由して、サーバに送信される。データの送信は図９と同様に、ＯＳ－９／ＯＳ－９００　０　３９上のダウンロードプロトコルであるUPLINK/DOWNLINK API ４０を使用し、ファイル・マネージャ、ドライバ３８によって、サーバ用のＯＳ３３を介して、ファイバーケーブル４２に接続されているハードウェア３７から、サーバへ送信される。サーバ側では、UPLINK/DOWNLINK API ３２を使用して、サーバ固有のネットワークドライバ３４を使用して、ハードウェア３５を介して接続されているファイバーケーブル４６からＡＴＭスイッチ４５を経由してデジタル双方向通信端末から送信されたデータを受信する。暗号化されたデータとデータ用暗号化鍵を受信したサーバは、まず自分の秘密鍵を使用してデータ用暗号化鍵を復号する。次に復号された暗号化鍵を使用して、データの復号を行う。復号されたデータはサーバ上の記憶領域に保存される。以上の動作により、デジタル双方向通信端末はサーバへデータを安全に送信することが可能となり、またデジタル双方向通信端末におけるデータの暗号化処理の必要回数を減らすことが可能となり、サーバへのデータ送信の効率を上げることが可能となる。

【０１３３】

【発明の効果】本発明は以上説明したように構成されているので、以下に示すような効果を奏する。

【０１３４】デジタル双方向通信端末にデジタル双方向通信システムのダウンロード機能を利用した暗号化機能の実現が可能となり、デジタル双方向通信端末に暗号化機能を実現することによって、よりセキュリティを必要とするサービスの提供が可能である。加えて、データと同様にアプリケーションをダウンロードすることが可能であり、更にダウンロードされたアプリケーションをダイナミックに動作可能とするＯＳ／９の特徴を利用することによって、デジタル双方向通信端末本体に特別な変更を加えることなく暗号化機能を付加することが可能となり、また暗号化機能の更新を容易に実現する。

【０１３５】また、デジタル双方向通信端末とサーバの間で授受されるデータを暗号化することによって、盗聴によるデータの保護は実現できるが、送った情報が途中で故意に変更され、送った内容と異なる内容が相手に届く恐れのあるデータの改ざん、第３者によって正当なユーザあるいはサーバのふりをして誤った情報をおくるなりすましの脅威は存在する。従って、認証機能のＨ／Ｗによる実装を行うことによって、データを改ざん、なりすましから保護し、よりセキュリティ機能の強化が実現できる。

【０１３６】また、認証機能のＳ／Ｗによる実装を行うことによって、より強化されたセキュリティ機能を実現しつつ、コストを削減できる。

【０１３７】また、データの保護機能を付加するための暗号化・復号化には複雑な演算が必要とされるため、特にセキュリティの確保を必要とするデータを選択的に暗号化・復号化する機能を付加することによって、デジタル双方向通信端末の負荷を軽減し、サーバとのデータ授受の速度を上げることができる。

【０１３８】また、データが暗号化・復号化を必要とするか否かをサーバ側で決定し、そのリストをデジタル双方向通信端末にダウンロードしてサーバ側と端末側で共通のリストによって、暗号化・復号化を選択的に実行する機能を有することによって、ユーザの操作が不要となり、ユーザの操作の煩雑さをなくすと共に、ユーザによる誤操作の危険性を回避する効果がある。さらに暗号化・復号化は共通なリストによって選択するため、データが暗号化されたものであるかどうかを示すフラグを送受信されるデータに付加する必要がなくなる。

【０１３９】また、デジタル双方向通信端末からサーバへ送信するデータで、暗号化されたものを保持しておくことによって、同じデータを何度も暗号化する必要がなくなり、デジタル双方向通信端末の負荷を軽減し、動作速度を上げることができる。

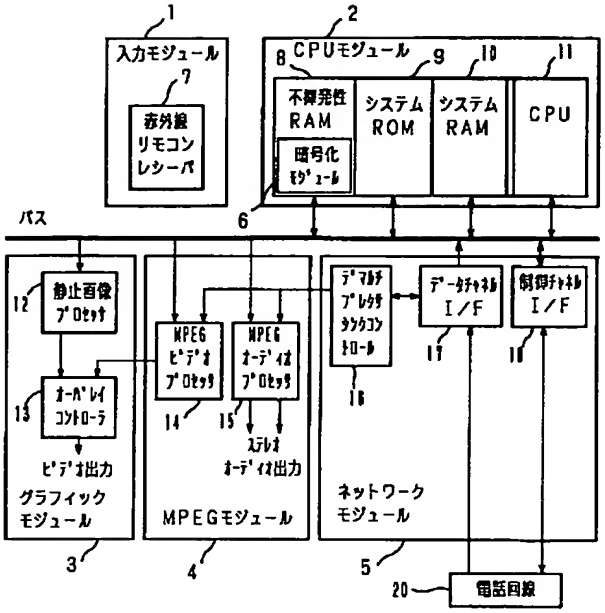
【図面の簡単な説明】

【図１】　本発明の実施の形態１であるシステム構成を示すブロック図である。

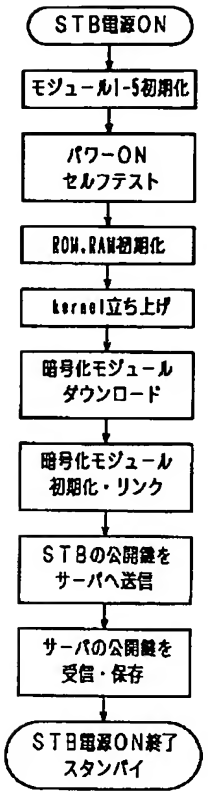
【図２】　デジタル双方向通信端末電源ＯＮ時のフロー

チャートである。
【図３】　データダウンロード時のフローチャートである。
【図４】　データ送信時のフローチャートである。
【図５】　電話回線を介したサーバとデジタル双方向通信端末の接続図である。
【図６】　本発明の実施の形態２であるシステム構成を示すブロック図である。
【図７】　ＨＦＣ方式によるサーバとデジタル双方向通信端末の接続図である。
【図８】　本発明の実施の形態３であるシステム構成を示すブロック図である。
【図９】　ＡＴＭによるサーバとデジタル双方向通信端末の接続図である。
【図１０】　本発明の実施の形態４であるシステム構成を示すブロック図である。
【図１１】　デジタル双方向通信端末電源ＯＮ時のフローチャートである。
【図１２】　データダウンロード時のフローチャートである。
【図１３】　データ送信時のフローチャートである。
【図１４】　本発明の実施の形態５であるシステム構成を示すブロック図である。
【図１５】　本発明の実施の形態６であるシステム構成を示すブロック図である。
【図１６】　本発明の実施の形態７であるシステム構成を示すブロック図である。
【図１７】　本発明の実施の形態８であるシステム構成を示すブロック図である。
【図１８】　本発明の実施の形態９であるシステム構成を示すブロック図である。
【図１９】　本発明の実施の形態１０であるシステム構成を示すブロック図である。
【図２０】　デジタル双方向通信端末電源ＯＮ時のフローチャートである。
【図２１】　データダウンロード時のフローチャートである。
【図２２】　データ送信時のフローチャートである。
【図２３】　本発明の実施の形態１１であるシステム構成を示すブロック図である。
【図２４】　本発明の実施の形態１２であるシステム構成を示すブロック図である。
【図２５】　本発明の実施の形態１３であるシステム構成を示すブロック図である。
【図２６】　デジタル双方向通信端末電源ＯＮ時のフローチャートである。
【図２７】　データダウンロード時のフローチャートである。
【図２８】　データ送信時のフローチャートである。
【図２９】　本発明の実施の形態１４であるシステム構成を示すブロック図である。
【図３０】　本発明の実施の形態１５であるシステム構成を示すブロック図である。
【図３１】　本発明の実施の形態１６であるシステム構成を示すブロック図である。
【図３２】　デジタル双方向通信端末電源ＯＮ時のフローチャートである。
【図３３】　データダウンロード時のフローチャートである。
【図３４】　データ送信時のフローチャートである。
【図３５】　本発明の実施の形態１７であるシステム構成を示すブロック図である。
【図３６】　本発明の実施例の形態１８であるシステム構成を示すブロック図である。
【図３７】　従来のＲＯＭのメモリマップである。
【図３８】　従来のデジタル双方向通信端末における電源ＯＮ時のフローチャートである。
【図３９】　従来のデジタル双方向通信端末におけるデータダウンロード時のフローチャートである。
【図４０】　ＯＳ／９を核とした従来のディジタル双方向通信端末の構成図である。
【符号の説明】
１　入力モジュール、２　ＣＰＵモジュール、３　グラフィックモジュール、４　ＭＰＥＧモジュール、５　ネットワークモジュール、６　暗号化モジュール、７　赤外線リモコンレシーバ、８　不揮発性ＲＡＭ、９　システムＲＯＭ、１０　システムＲＡＭ、１１　ＣＰＵ、１２　静止画像プロセッサ、１３　オーバレイコントローラ、１４　ＭＰＥＧビデオプロセッサ、１５　ＭＰＥＧオーディオプロセッサ、１６　デマルチプレクサコントロール、１７　データチャネルＩ／Ｆ、１８　制御チャネルＩ／Ｆ。

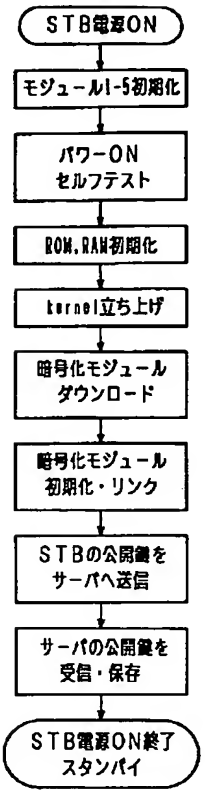
【図１】



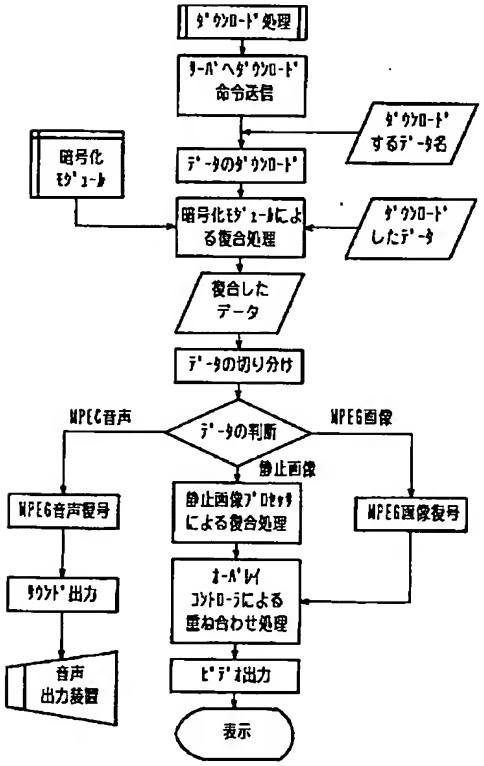
【図２】



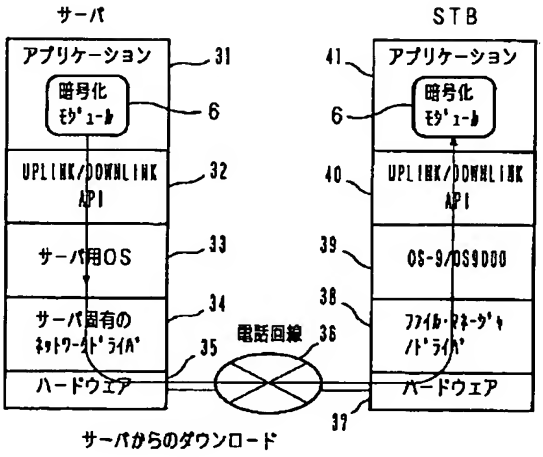
【図２０】



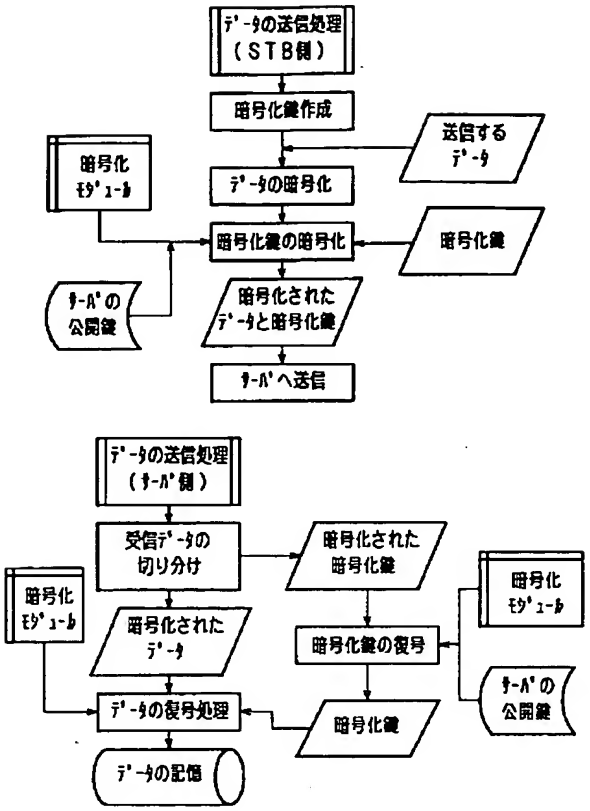
【図３】



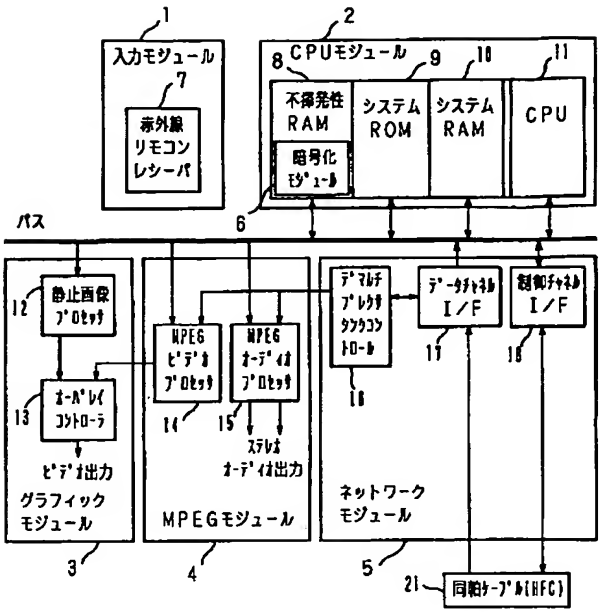
【図５】



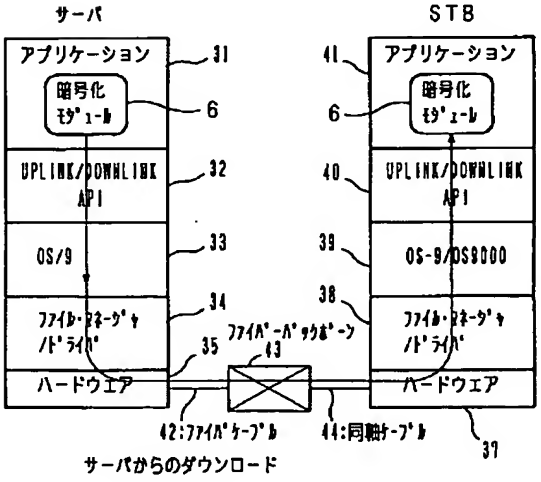
【図４】


データの送信処理
（STB側）
暗号化鍵作成
送信する
データ
暗号化
モジュール
データの暗号化
暗号化鍵の暗号化
暗号化鍵
サーバの
公開鍵
暗号化された
データと暗号化鍵
サーバへ送信
データの送信処理
（サーバ側）
受信データの
切り分け
暗号化された
暗号化鍵
暗号化
モジュール
暗号化
モジュール
暗号化された
データ
暗号化鍵の復号
データの復号処理
暗号化鍵
サーバの
公開鍵
データの記憶

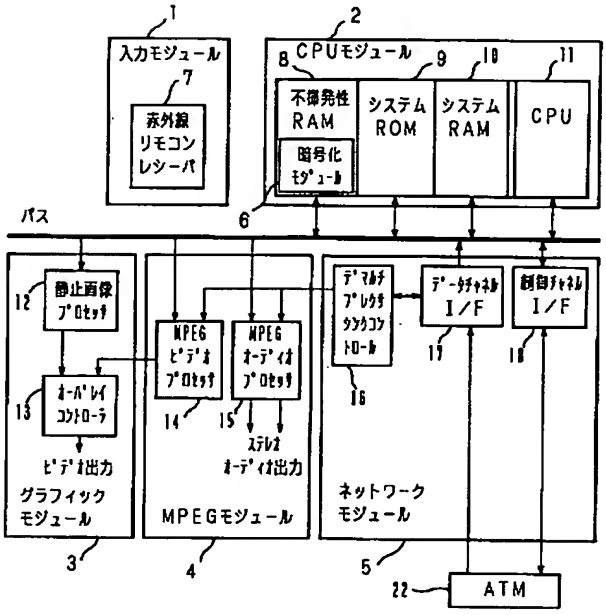
【図６】


入力モジュール
CPUモジュール
赤外線
リモコン
レシーバ
不揮発性
RAM
暗号化
モジュール
システム
ROM
システム
RAM
CPU
バス
静止画像
プロセッサ
MPEG
ビデオ
プロセッサ
MPEG
オーディオ
プロセッサ
オーバレイ
コントローラ
ビデオ出力
ステレオ
オーディオ出力
グラフィック
モジュール
MPEGモジュール
ネットワーク
モジュール
I／F
同軸ケーブル(HFC)

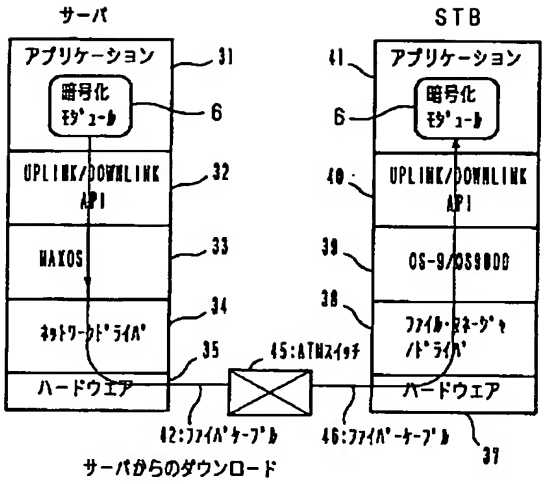
【図７】


サーバ
STB
アプリケーション
暗号化
モジュール
UPLINK/DOWNLINK
API
OS/9
OS-9/OS9000
ファイル・ネットワーク
ドライバ
ハードウエア
ファイバーバックボーン
42:ファイバーケーブル
44:同軸ケーブル
サーバからのダウンロード

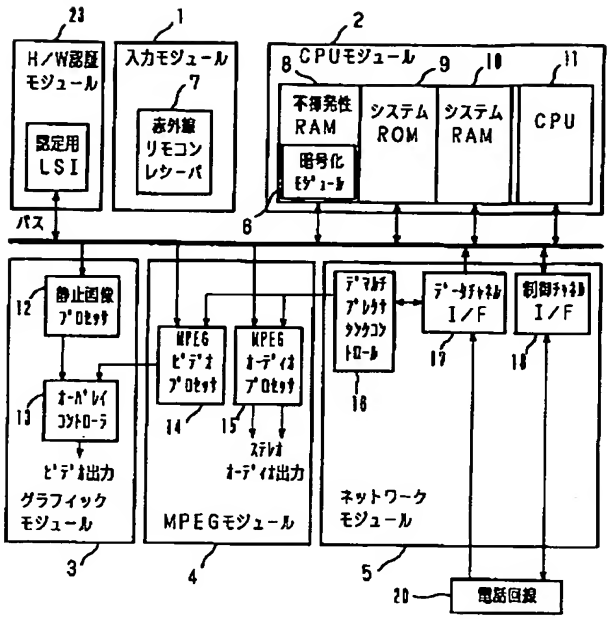
【図８】


入力モジュール
CPUモジュール
赤外線
リモコン
レシーバ
不揮発性
RAM
暗号化
モジュール
システム
ROM
システム
RAM
CPU
バス
静止画像
プロセッサ
MPEG
ビデオ
プロセッサ
MPEG
オーディオ
プロセッサ
オーバレイ
コントローラ
ビデオ出力
ステレオ
オーディオ出力
グラフィック
モジュール
MPEGモジュール
ネットワーク
モジュール
I／F
ATM

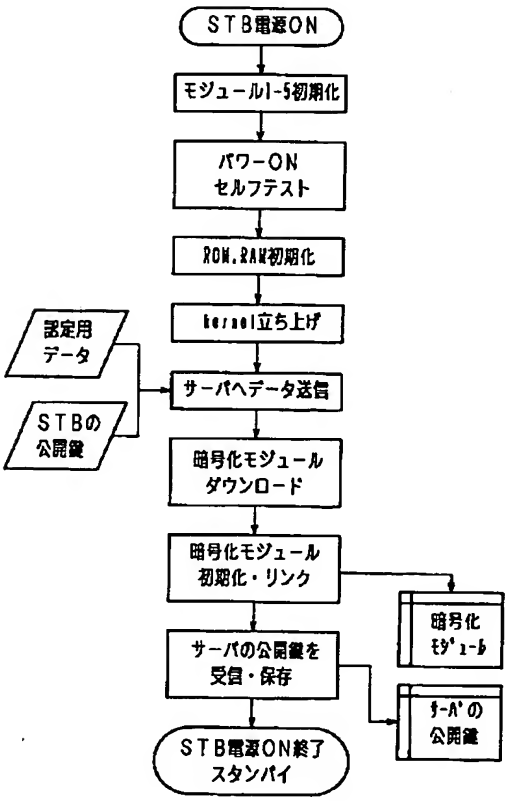
【図９】



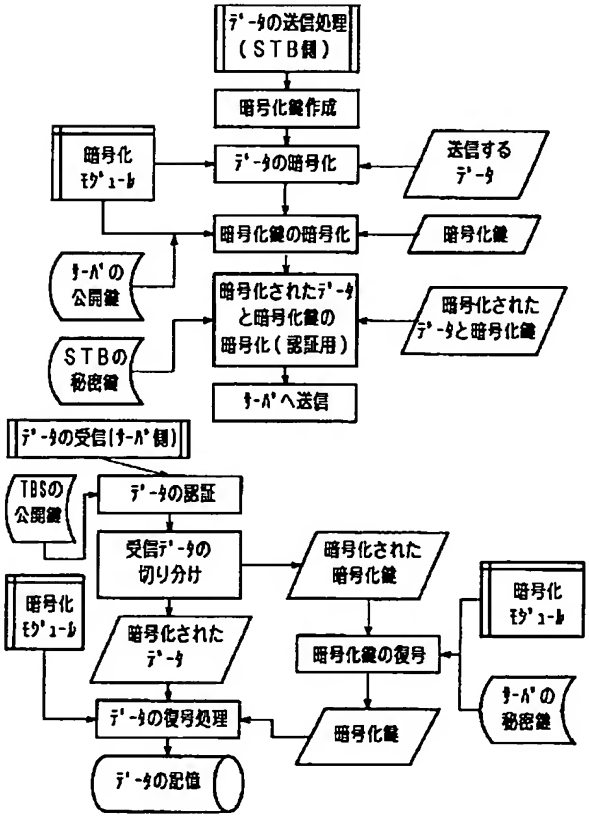
【図１０】



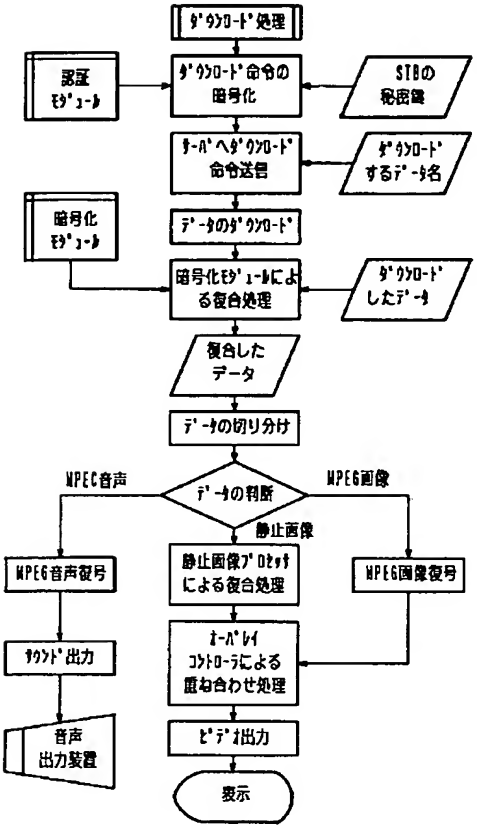
【図１１】



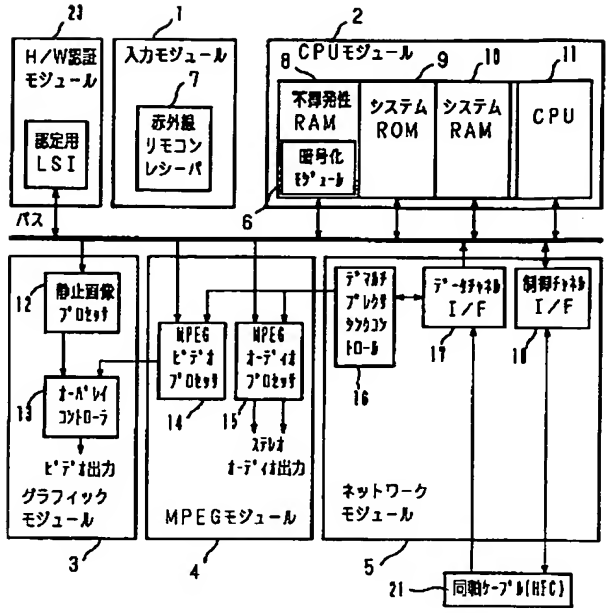
【図１３】



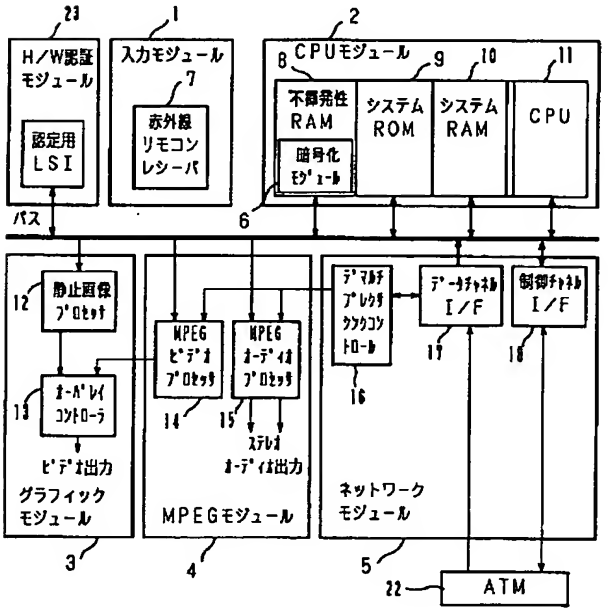
【図１２】


ﾀﾞｳﾝﾛｰﾄﾞ処理
認証 ﾓｼﾞｭｰﾙ
ﾀﾞｳﾝﾛｰﾄﾞ命令の暗号化
STBの秘密鍵
ｻｰﾊﾞへﾀﾞｳﾝﾛｰﾄﾞ命令送信
ﾀﾞｳﾝﾛｰﾄﾞするﾃﾞｰﾀ名
暗号化 ﾓｼﾞｭｰﾙ
ﾃﾞｰﾀのﾀﾞｳﾝﾛｰﾄﾞ
暗号化ﾓｼﾞｭｰﾙによる復合処理
ﾀﾞｳﾝﾛｰﾄﾞしたﾃﾞｰﾀ
復合したデータ
ﾃﾞｰﾀの切り分け
MPEG音声
ﾃﾞｰﾀの判断
MPEG画像
静止画像
MPEG音声復号
静止画像ﾌﾟﾛｾｯｻによる復合処理
MPEG画像復号
ｻｳﾝﾄﾞ出力
ｵｰﾊﾞﾚｲ ｺﾝﾄﾛｰﾗによる重ね合わせ処理
音声出力装置
ﾋﾞﾃﾞｵ出力
表示

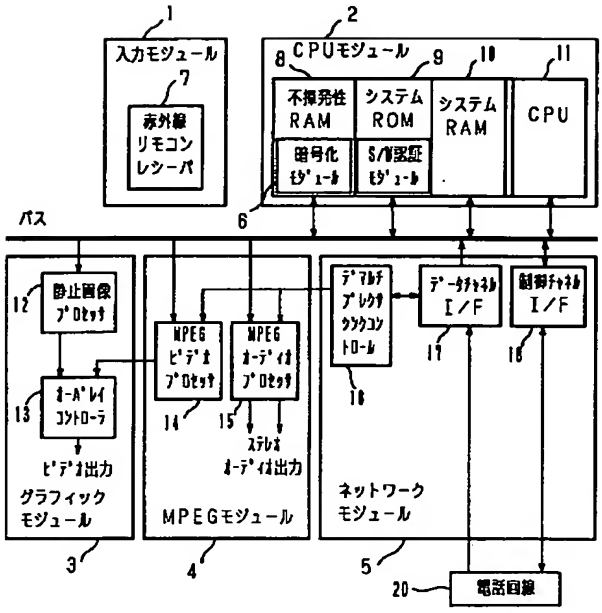
【図１４】


23
H/W認証モジュール
認定用LSI
1
入力モジュール
7
赤外線リモコンレシーバ
2
CPUモジュール
8
不揮発性RAM
暗号化ﾓｼﾞｭｰﾙ
9
システムROM
10
システムRAM
11
CPU
6
バス
12
静止画像ﾌﾟﾛｾｯｻ
13
ｵｰﾊﾞﾚｲ ｺﾝﾄﾛｰﾗ
ﾋﾞﾃﾞｵ出力
グラフィックモジュール
3
MPEG ﾋﾞﾃﾞｵ ﾌﾟﾛｾｯｻ
14
MPEG ｵｰﾃﾞｨｵ ﾌﾟﾛｾｯｻ
15
ｽﾃﾚｵ ｵｰﾃﾞｨｵ出力
MPEGモジュール
4
ﾏﾙﾁﾌﾟﾚｸｻｺﾝﾄﾛｰﾗ
16
ﾃﾞｰﾀﾁｬﾈﾙ I/F
17
制御ﾁｬﾈﾙ I/F
18
ネットワークモジュール
5
21
同軸ｹｰﾌﾞﾙ(HFC)

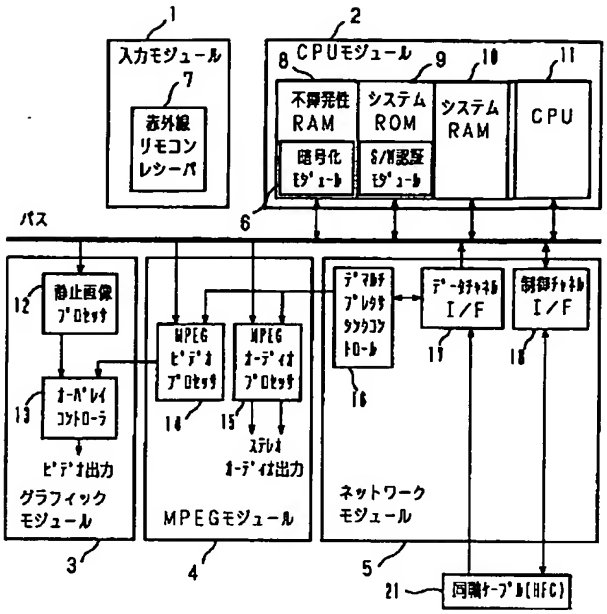
【図１５】


23
H/W認証モジュール
認定用LSI
1
入力モジュール
7
赤外線リモコンレシーバ
2
CPUモジュール
8
不揮発性RAM
暗号化ﾓｼﾞｭｰﾙ
9
システムROM
10
システムRAM
11
CPU
6
バス
12
静止画像ﾌﾟﾛｾｯｻ
13
ｵｰﾊﾞﾚｲ ｺﾝﾄﾛｰﾗ
ﾋﾞﾃﾞｵ出力
グラフィックモジュール
3
MPEG ﾋﾞﾃﾞｵ ﾌﾟﾛｾｯｻ
14
MPEG ｵｰﾃﾞｨｵ ﾌﾟﾛｾｯｻ
15
ｽﾃﾚｵ ｵｰﾃﾞｨｵ出力
MPEGモジュール
4
ﾏﾙﾁﾌﾟﾚｸｻｺﾝﾄﾛｰﾗ
16
ﾃﾞｰﾀﾁｬﾈﾙ I/F
17
制御ﾁｬﾈﾙ I/F
18
ネットワークモジュール
5
22
ATM

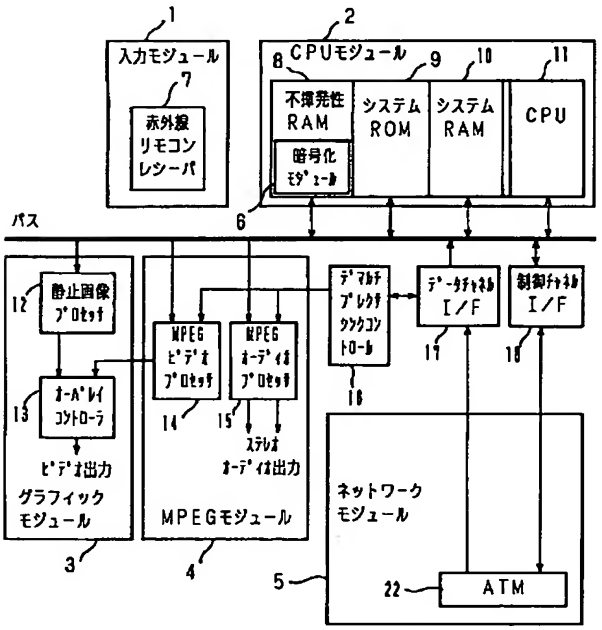
【図１６】



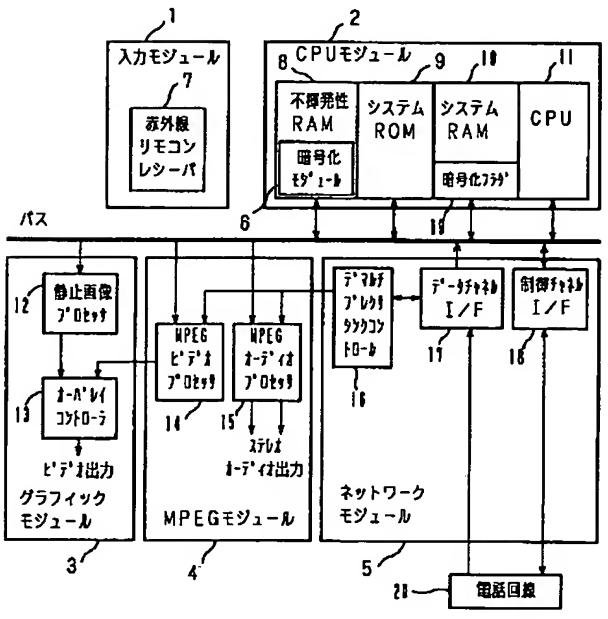
【図１７】



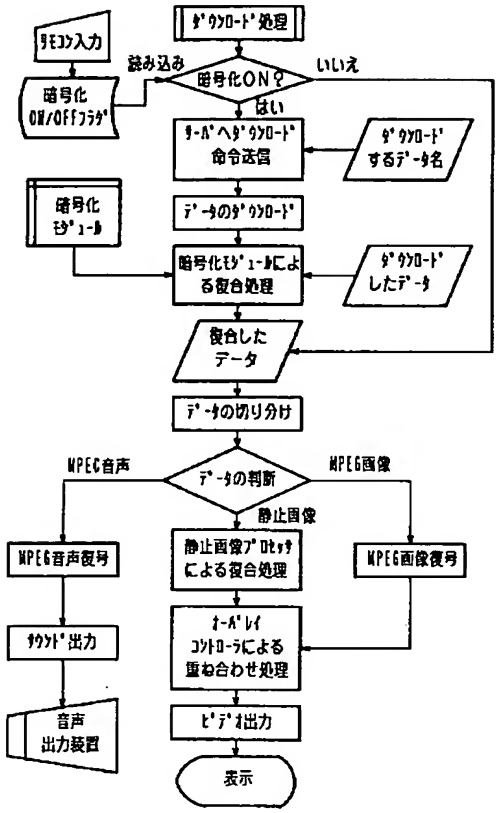
【図１８】



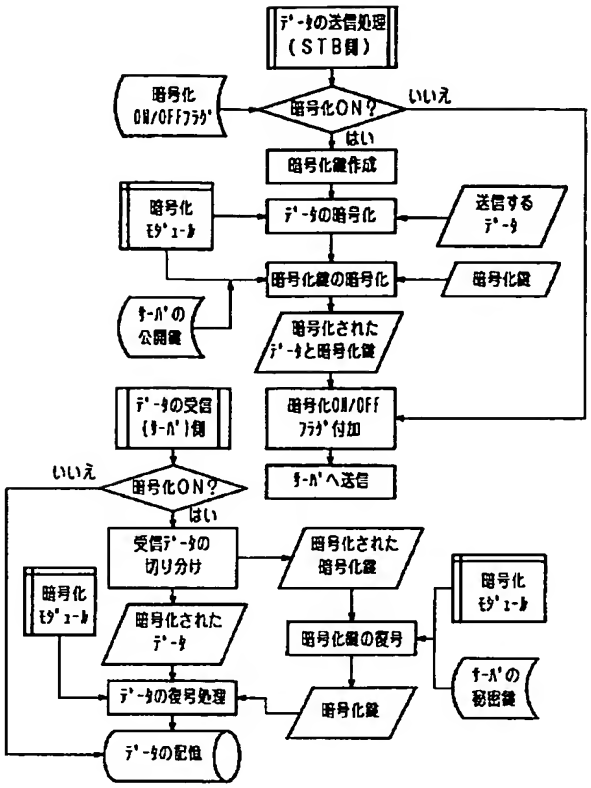
【図１９】



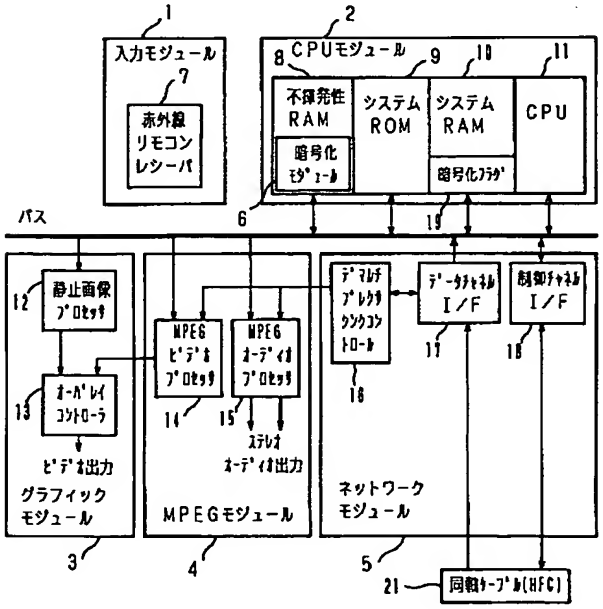
【図２１】



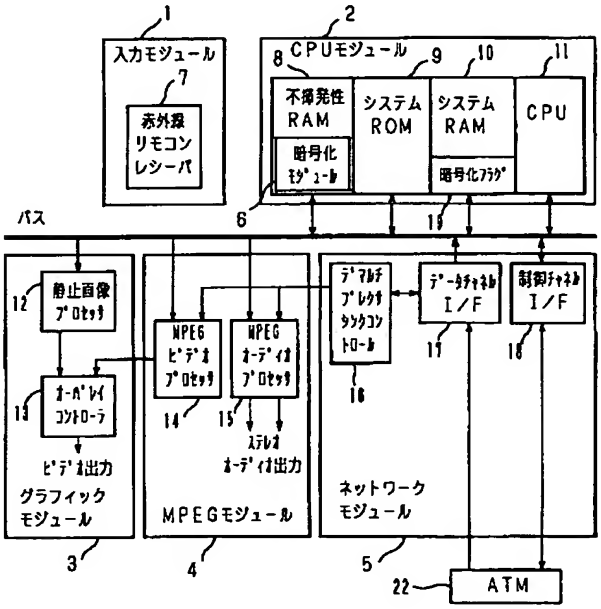
【図２２】



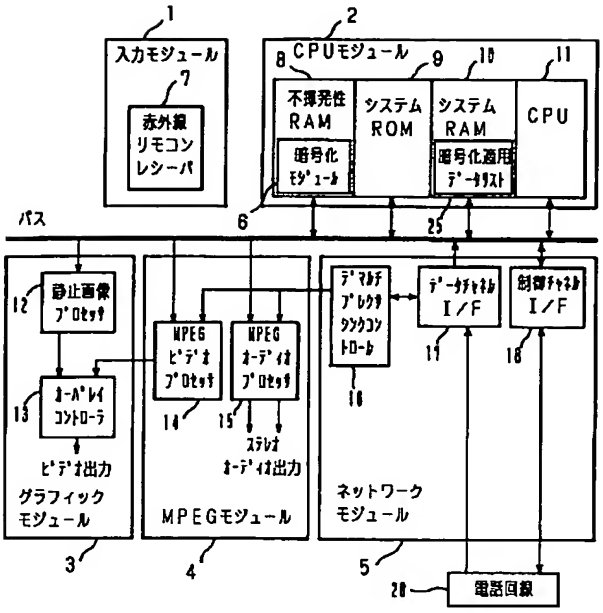
【図２３】



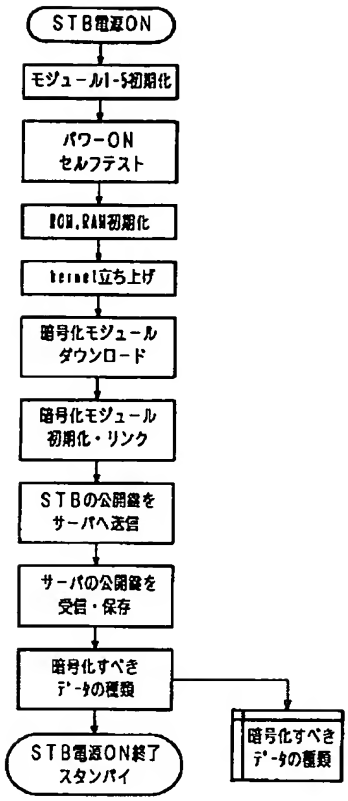
【図２４】



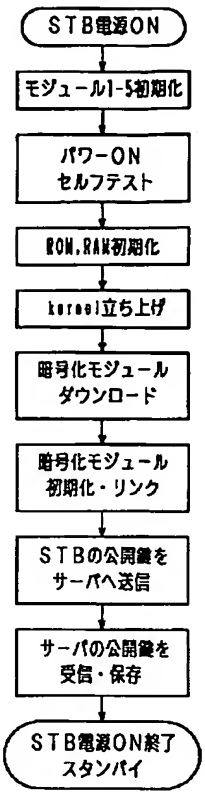
【図２５】



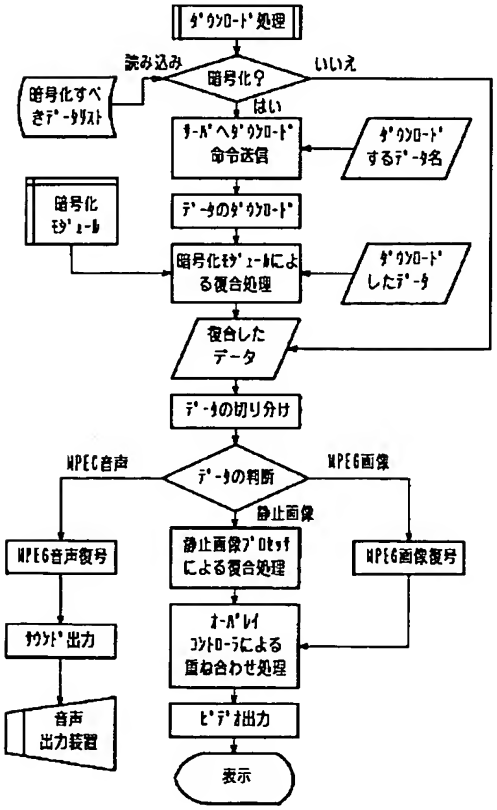
【図２６】



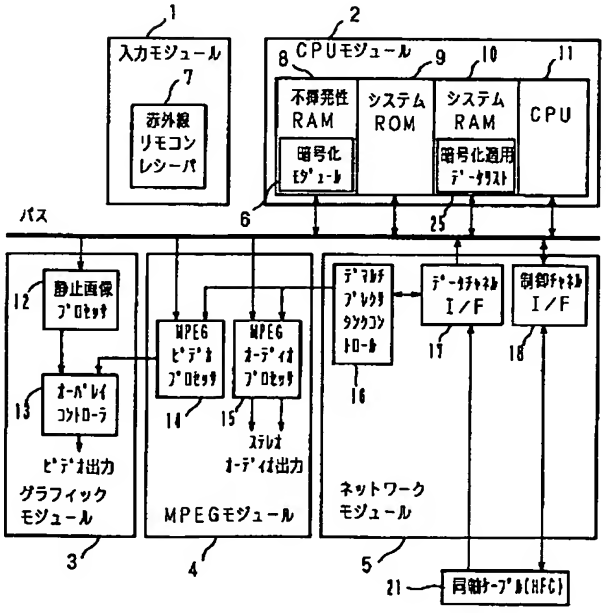
【図３２】



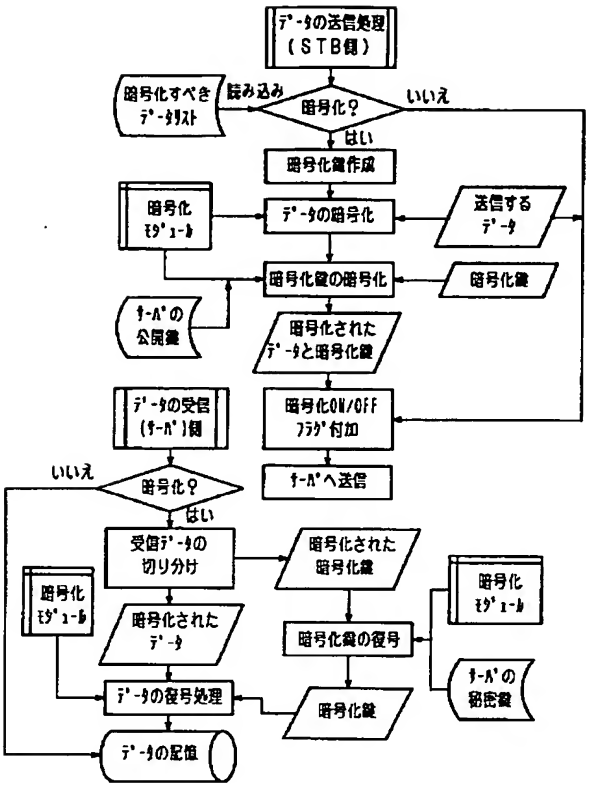
【図２７】



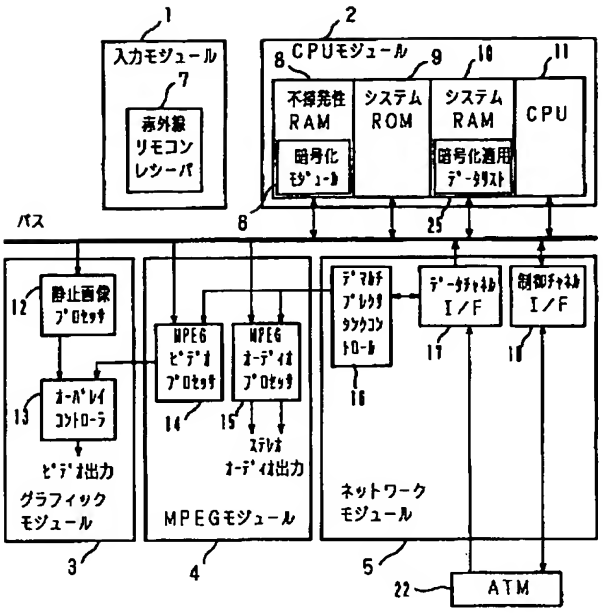
【図２９】



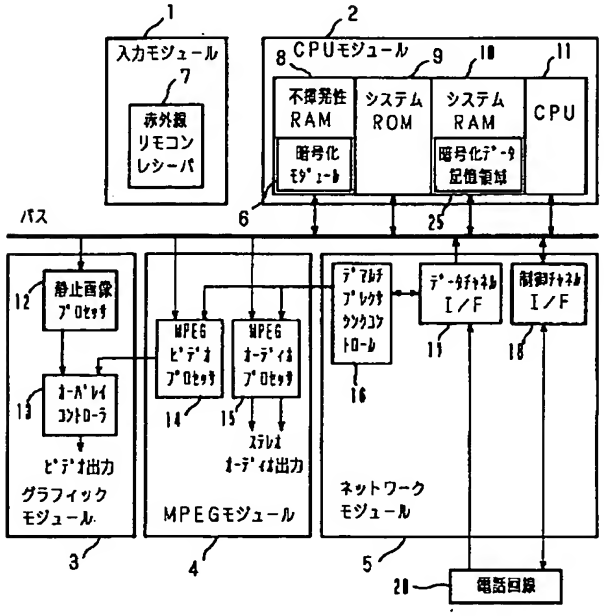
【図２８】



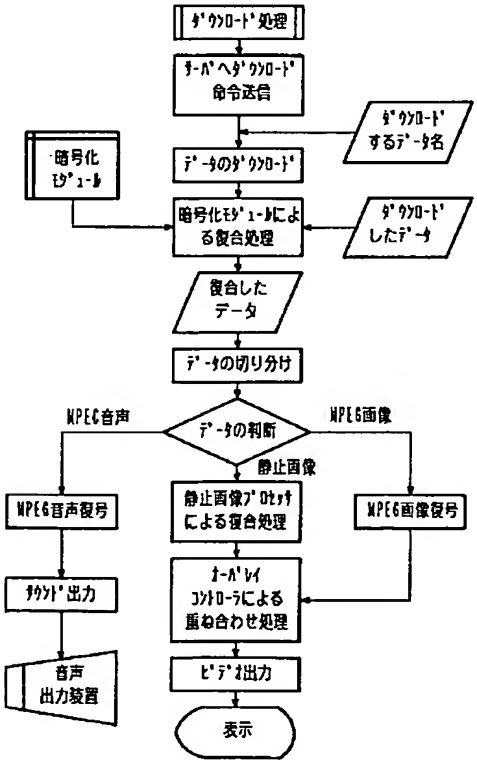
【図３０】



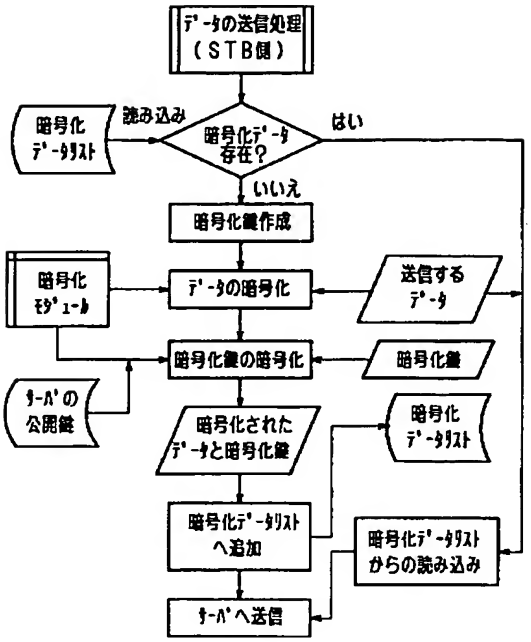
【図３１】



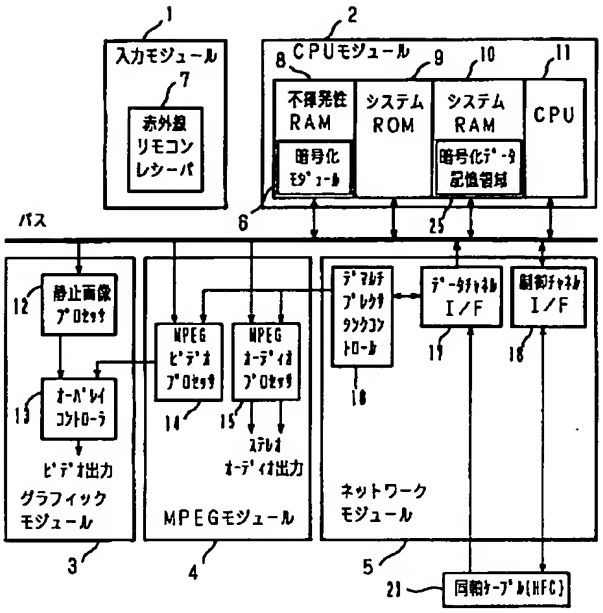
【図３３】



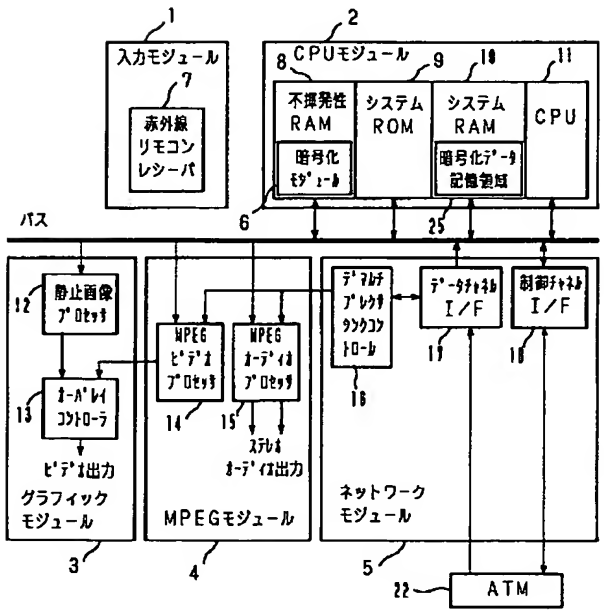
【図３４】



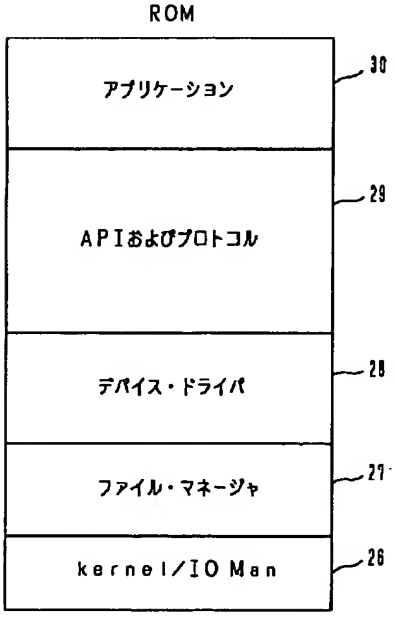
【図３５】



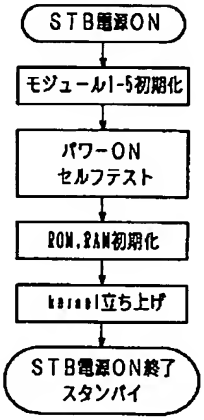
【図３６】



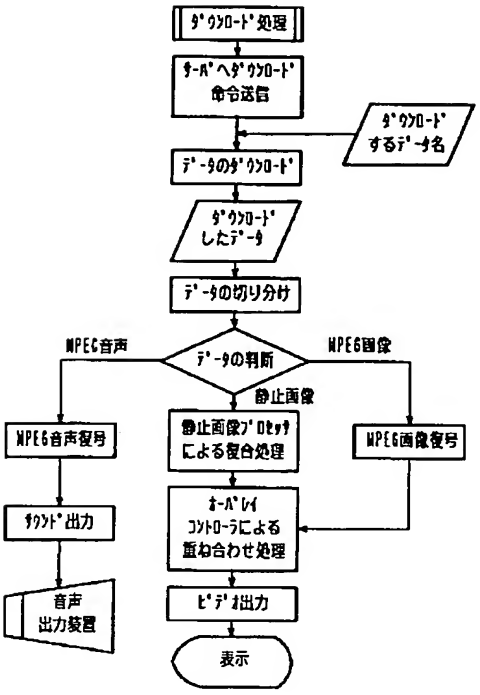
【図３７】



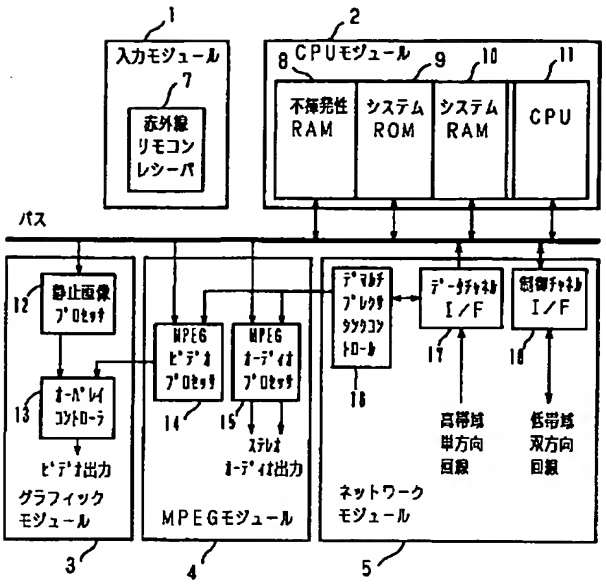
【図３８】



【図３９】



【図４０】



フロントページの続き

(51)Int.Cl.⁶		識別記号	庁内整理番号	FI		技術表示箇所
G09C	1/00	660	7259－5J	G09C	1/00	660E
H04H	1/02			H04H	1/02	E
						F
H04L	9/08			H04N	7/14	
	9/32			H04L	9/00	601C
H04N	7/14					601E
	7/167					675B
				H04N	7/167	Z